This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 697 491 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.02.1996 Bulletin 1996/08

(51) Int. Cl.[6]: **E05B 49/00**

(21) Application number: **95112156.5**

(22) Date of filing: **02.08.1995**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **05.08.1994 JP 184849/94**
03.07.1995 JP 167434/95

(71) Applicant: **NIPPONDENSO CO., LTD.**
Kariya-city Aichi-pref., 448 (JP)

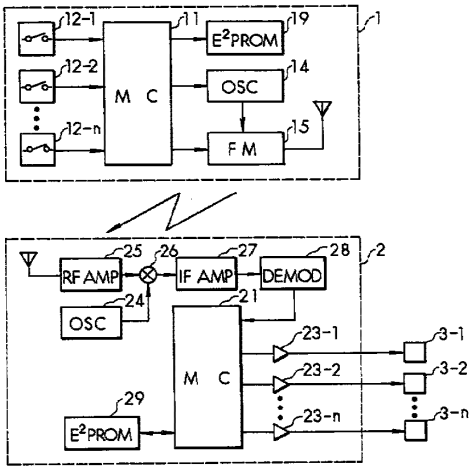
(72) Inventors:
- **Mabuchi, Tomoji**
  Kariya-city, Aichi-pref. (JP)
- **Hotta, Hisataka**
  Gifu-city, Gifu-pref. (JP)

(74) Representative: **KUHNEN, WACKER & PARTNER**
D-85354 Freising (DE)

(54) Remote control system and method using variable ID code

(57) In a remote control system, each time a transmission code is transmitted, a rolling code (R2-R0) having a prescribed bit configuration is cumulatively varied (S30). An operation process (S40) is performed between each bit data item of the rolling code and each corresponding bit data item of the ID code (I5-I0), whereby each bit data item of the ID code is varied in correspondence with the rolling code, thus setting a variable ID code. Since the ID code itself which is contained in the signal is also varied in correspondence with the variable code, the fixed portion contained in the signal is decreased with the result that the ID code is almost infinitely widely varied. Accordingly, it becomes almost impossible to decode the ID code even if it is intercepted.

FIG. 1



EP 0 697 491 A1

Printed by Rank Xerox (UK) Business Services
2.9.9/3.4

WAVELYNX EX. 1003, Pg. 1369
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Description

CROSS REFERENCE TO RELATED APPLICATIONS

This application is based on and claims priorities of Japanese Patent Applications No. 6-184849 filed August 5, 1994 and No. 7-167434 filed July 3, 1995, the contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention:

The present invention relates to a remote control system and method which uses a variable ID (identification) code and is used in, for example, a protection system such as a wireless door lock control system for a vehicle.

2. Description of Related Art:

Conventionally, in a remote control system which is adopted in, for example, a wireless door lock control system, an individual ID code is set in a coded signal transmitted and received through radiocommunication, and the coded signal containing this ID code is transmitted from a transmitter. The transmitted coded signal is received by a receiver, and the ID code contained in the received coded signal and an ID code preset in the receiver are compared with each other. Then, when both ID codes coincide with each other, the system operates the object to be controlled to thereby prevent another from using the ID code signal.

However, it has in recent years been reported that the above ID code can be copied by an interceptor device which intercepts an ID code contained in the coded signal transmitted through radiocommunication, and that an unauthorized person other than the authorized user can use the signal without authorization by transmitting the same ID code. This means that the security of the conventional type of remote control system directed only to transmitting and receiving an individual ID code can be breached.

As a countermeasure against this, for example, Japanese Unexamined Patent Application Laid-open No. H1-278671 discloses a remote control system which comprises, in addition to a fixed ID code, a code-number cumulative alteration means for cumulatively altering the code number in correspondence with the transmission frequency according to a prescribed sequential order. Namely, in the remote control system disclosed in the above publication, a code number (rolling code) which is altered in correspondence with the transmission frequency according to a prescribed sequential order is added, in addition to the ID code, to the transmission code, and this code number is utilized for judgement of a transmission signal. For this reason, even if the transmission signal is copied by the transmission signal interceptor device, mere transmission of such copied signal cannot use the ID code signal because code information is altered for each transmission and this altered information is utilized for determination of the transmission signal.

However, in the conventional system, although the system is comprised of a variable code number, the ID code per se that is fixed is still contained in the transmission signal. Therefore, if the transmission signal is intercepted many times by the ID code interceptor device, decoding thereof will be possible by determining that the code which is continuously fixed is the ID code and the varying code is the rolling code and by finding the regularity in the variation of the varying code. Namely, since the information of the ID code which is fixed exists in the transmission signal, an unauthorized person who uses it without authorization can relatively easily determine what portion of the signal is the ID code and what portion of the signal is the rolling code. Further, if the regularity of a variable portion of the code other than the ID code has been found after noticing this variable portion, the unauthorized user would be able to use the ID code signal.

SUMMARY OF THE INVENTION

The present invention has an object to provide a remote control system in which the ID code itself which is contained in a signal is also varied in correspondence with a variable code to thereby substantially eliminate a fixed code portion in the signal, thus increasing the difficulty of intercepting and decoding the signal.

According to the present invention, in a remote control system, each time a transmission code is transmitted, a rolling code composed of a prescribed number of bits is cumulatively varied. Then, each bit data item of the rolling code and each corresponding bit data item of an ID code are operation processed thereby to vary each bit data item of the ID code in correspondence with the rolling code, thus setting a variable ID code. Namely, the ID code in the transmission signal is also varied in correspondence with the rolling code and therefore substantially the entire information in the transmission signal is variable information. Thus, what portion of the signal is the ID code and what portion thereof is the rolling code cannot be discriminated. Further, it is almost impossible to find a regularity in the variation of the rolling code. Accordingly, it is possible to prevent an unauthorized person other than the authorized user from using the signal without authorization.

Preferably, the variable ID code is set by combining the bits of the rolling code in the same number as that of the bits of the ID code according to a prescribed combination setting and performing an exclusive-OR operation between each bit data item of the combined rolling code and each corresponding bit data item of the ID code. Namely, by utilizing the exclusive-OR operation, coding and decoding processes are more efficiently performed compared with various other operation processes.

WAVELYNX EX. 1003, Pg. 1370
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Further, the rolling code is cumulatively varied and the restored rolling code and the rolling code reset in a receiver are compared with each other for determining whether or not the rolling code is correct. Namely, since the degree of coincidence between both rolling codes as well as that between both ID codes is determined by comparison, the level of security is excellent. In the case where it has been determined that the restored rolling code is correct, the following effect is brought about by storing the restored rolling code. That is, even when the rolling code of the transmitter has preceded the rolling code of the receiver (for example, where the rolling code has not been received despite having been transmitted), a correspondence therebetween can be attained.

Preferably, a plurality of kinds of bit-data rearranging order settings are provided as the prescribed bit-data rearranging order settings. Although a larger space is needed as the memory space since a plurality of kinds are set, the transmission code is varied in a more complex manner, whereby the difficulty of decoding increases. Further, if the prescribed bit-data rearranging order setting is selected by a random number, the transmission code cannot be decoded unless a relevant random number is obtained.

More preferably, it is determined whether or not a prescribed time period has passed from the start of transmission. Where it has been determined that the transmission time period is not longer than the prescribed time period, the bit data items are rearranged according to a relevant prescribed bit-data rearranging order setting as preset, and the rearranged code is stopped from being added to the transmission code. Where it has been determined that the transmission time period is longer than such prescribed time period, the relevant prescribed bit-data rearranging order setting is updated and the bit data items are rearranged according to this updated prescribed bit-data rearranging order setting, and the updated rearranged code is added to the transmission code. In other words, only when the transmission code has continued to be transmitted for at least the prescribed time period, the relevant prescribed bit-data rearranging order setting is updated. As a result, by appropriately changing the transmission time period, the user can freely change the bit-data rearranging order setting. In addition, if the user changes this once, he can prevent the rearranged code from being added to the transmission code from the next time onward only if the transmission time period is not longer than the prescribed time period. Therefore, the transmission code has no information due to the bit-data rearrangement, so that even if the transmission code has been intercepted, decoding thereof becomes virtually impossible.

BRIEF DESCRIPTION OF THE DRAWINGS

In the accompanying drawings:

Fig. 1 is a schematic structural diagram illustrating an embodiment of the present invention;

Figs. 2A and 2B are flowcharts illustrating operations of a transmitter and a receiver illustrated in Fig. 1, respectively;

Fig. 3 is a schematic view illustrating states of codes at a transmission-code composing time;

Fig. 4 is a table illustrating patterns according to which the orders of bit-position rearrangement are set;

Fig. 5 is a schematic view illustrating states of codes at the transmission-code decoding time;

Fig. 6 is a flow chart illustrating the operation of the transmitter, in the case where a sorting code is added after the passage of a prescribed time period;

Fig. 7 is a flow chart illustrating the operation of the receiver, in the case where a sorting code is added after the passage of a prescribed time period; and

Fig. 8 is a table illustrating patterns according to which the bit-position combinations are set.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described hereafter with reference to the embodiments illustrated in the drawings.

[First Embodiment]

Fig. 1 is a structural diagram representing a remote control system (transmission and reception system) which is applied to a protection system such as, for example, a wireless door lock control system for a vehicle.

In Fig. 1, reference numeral 1 denotes a transmitter, in which there are provided switches 12-1, 12-2, ---, 12-n for performing remote control operations on their respective different functions (for example, door lock, opening/closing of trunk, seat position setting, etc.). Signals generated as a result of the switch operations are input to a microprocessor (MC) 11. To this microprocessor 11 there is connected an EEPROM 19, in which there is stored an ID code specific to the transmitter 1. RAM (not illustrated) is formed in the microprocessor 11 and this RAM stores a rolling code the content of the information of which varies each time it is transmitted, as well as with data for transmission code production. Further, an oscillator circuit 14 and an FM modulator circuit 15 are connected to the microprocessor 11 so as to FM modulate a transmission code produced in the microprocessor 11 and transmit it from an antenna.

Meanwhile, a receiver 2 is provided with receiver circuitry for demodulating the transmitted signal from the transmitter 1, which receiver circuitry is formed by a radio frequency amplifier circuit 25, local oscillator 24, mixer circuit 26, intermediate frequency amplifier circuit 27, and demodulator circuit 28. The output signal as demodulated by this receiver circuitry 2 is input to a microprocessor 21. This microprocessor 21 produces an ID code and rolling code from the output signal as demodulated

WAVELYNX EX. 1003, Pg. 1371
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

according to previously determined processes. An EEPROM 29 which stores a code corresponding to the ID code specific to the transmitter 1 is connected to the microprocessor 21. Further, control objects 3-1, 3-2, ---, 3-n (for example, actuators for performing door locking, trunk opening/closing, seat position setting, etc.) are connected to the microprocessor 21 via drive circuits 23-1, 23-2, ---, 23-n, respectively. The control objects 3-1, 3-2, ---, 3-n are operated according to signals from the microprocessor 21.

Next, operation of the transmitter 1 and receiver 2 will be described according to the flow charts illustrated in Figs. 2A and 2B. The processes illustrated in the flowchart are processes which are executed by the microprocessors 11 and 21 respectively provided in the transmitter 1 and receiver 2.

Firstly, the operation of the transmitter 1 will be explained. In step 10, the operation is in standby until it is determined that any one of the switches 12-1 through 12-n has been operated, and when it is determined that any one of such switches has been operated, the operation proceeds to step 20. In step 20, a 4-bit random number (C3, C2, C1, C0) is generated and a bit-data rearranging order corresponding to the thus generated 4-bit random number is set according to the contents of a table shown in Fig. 4. In this embodiment, it is assumed that, for example, a 4-bit random number (0, 0, 0, 0) has been generated and an uppermost stage pattern shown in the table in Fig. 4 has been set for the bit-data rearranging order.

Next, in step 30, updating of the rolling code is performed. This rolling code is a variable composed of n bits (Rn-1 to R0), which variable is updated each time the rolling code is transmitted. Although in this embodiment it is assumed that the rolling code is a variable composed of 3 bits (1, 0, 0) and varies by +1 each time it is transmitted, the present invention is not limited thereto but any manner of variation may be available as long as the rolling code varies in accordance with a prescribed rule.

Further, in step 40, exclusive-OR operation is performed between the rolling code and the ID code. Specifically, as illustrated in Fig. 3, a previously determined bit combination (with no regularity), e.g. a 6-bit combination (R1, R2, R1, R0, R0, R2) is set for the rolling code, whereby exclusive-OR operation is performed between each bit value thereof and each corresponding bit value of the ID code. The ID code is a code specific to the transmitter 1 and stored in EEPROM 19 as mentioned above and that this ID code is a fixed value composed of m bits (Im-1 to I0). In this embodiment, a 6-bit value (0, 0, 1, 0, 1, 1) is set for this ID code. Therefore, in step 40, exclusive-OR operation is performed between the ID code (0, 0, 1, 0, 1, 1) and the combination rolling code (0, 1, 0, 0, 0, 1), so that an exclusive-OR of (0, 1, 1, 0, 1, 0) is set.

Next, in step 50, the exclusive-OR result set in step 40 and the rolling code are rearranged according to the bit-data rearranging order set in step 20. Specifically, as illustrated in Fig. 3, the (0, 1, 1, 0, 1, 0) and (1, 0, 0) are rearranged according to the bit-data rearranging order (I'3, R2, I'0, R0, I'2, I'5, R1, I'4, I'1), whereby (1, 1, 0, 0, 0, 0, 0, 1, 1) is set.

Next, in step 60, format bits (start bits, stop bits), function bits, and a parity bit are added to the code rearranged in step 50 and further the 4-bit random number (C3, C2, C1, C0) is added to thereby compose a transmission code. Specifically, as illustrated in Figs. 3 and 4, stop bits are disposed and then the rearranged code is disposed in such a manner as to be sectioned by the start bits. Further, the function bits, parity bit, and 4-bit random number (which indicates information on the bit-data rearranging order) are added to thereby compose a transmission code. The format bits are those for synchronizing data transmission while, on the other hand, the function bits (K1, K0) are those which represent which one of the operation switches has been operated. The parity bit is one for detecting a transmission error.

Next, in step 70, the transmission code which has been composed in step 60 is output to the FM modulator circuit 15. As a result, the transmission code is FM modulated and transmitted to the exterior of the transmitter 1 as a feeble wave.

The above-mentioned series of steps are intended for performing the processes to be executed in the transmitter 1 when one of the operation switches has been once operated. Therefore, when that operation switch is again depressed, the processes in steps 20 through 70 are again executed and, in this case, the 4-bit random number and the rolling code are changed. The transmission code to be transmitted next is illustrated in the simplified manner in the lower portion of Fig. 3A, provided, however, it is assumed that the 4-bit random number is identical.

Next, the operation of the receiver 2 will be explained with reference to Fig. 2B. In step 110, the operation is in standby until the transmission code from the transmitter 1 is received by the receiver 2. When the transmission code has been received, the operation proceeds to step 120. In step 120, the function bits, rearranged code (exclusive-ORed code + rolling code), and 4-bit random number which have been disposed at their respective prescribed positions are respectively drawn away from the transmission code, whereupon the rearranged code is restored to its original arrangement order according to the 4-bit random number, to restore the exclusive-ORed code and the rolling code. Specifically, as illustrated in Fig. 5, the rearranged code (1, 1, 0, 0, 0, 0, 0, 1, 1) is restored to its original arrangement order according to the 4-bit random number (0, 0, 0, 0) to restore the exclusive-ORed code (0, 1, 1, 0, 1, 0) and the rolling code (1, 0, 0).

Next, in step 130, the above-mentioned exclusive-ORed code is subjected to exclusive-OR operation by using the rolling code to restore the ID code. Specifically, as illustrated in Fig. 5, exclusive-OR operation is performed between each bit value of the same rolling code bit combination as that exclusive-ORed in step 40, i.e. 6-bit combination (R1, R2, R1, R0, R0, R2) and each corresponding bit value of the exclusive-ORed code.

WAVELYNX EX. 1003, Pg. 1372
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Namely, the ID code (0, 0, 1, 0, 1, 1) is restored from the exclusive-ORed code (0, 1, 1, 0, 1, 0) and the bit values of the 6-bit combination value (0, 0, 1, 0, 1, 1). It is assumed that the same 6-bit combination rolling code is set in both the transmitter 1 and the receiver 2.

Next, in step 140, it is determined whether or not the ID code set in the EEPROM 29 and the ID code of the transmission code restored in step 130 coincide with each other. If both coincide, the operation proceeds to step 150. If there is no coincidence between the codes, the operation returns to step 110 in which the operation is placed in standby.

Further, in step 150, comparing the rolling code restored in step 120 with the previously stored rolling code, it is determined whether or not the amount of change of the restored rolling code relative to the previous rolling code is in a range of from +1 to +X. If the amount of change is in this range, it is determined that the present rolling code is correct. Thus, the operation proceeds to step 160. If the amount of change is outside the range, the operation proceeds to step 110 in which the operation is placed in standby. At this time, if the transmission code from the transmitter 1 is received by the receiver 2 each time it is transmitted, the amount of change of the rolling code to be determined by comparison in the receiver 2 may be limited to the value of the previous rolling code plus 1. However, since in the case where the transmitter is operated without being accompanied by reception of the transmission code by the receiver 2, only the rolling code on the transmitter 1 is updated, such a permissible range is provided which could cope with such a case as well. Namely, assuming that the value of the rolling code restored from the transmission code is represented by ri and the value of the previous rolling code is represented by ri-1, if "$ri-1 + 1 \leqq ri \leqq ri-1 + X$", it is determined that the rolling code is normal.

Next, in step 160, the rolling code restored from the transmission code is stored in a RAM and the rolling code as stored is updated thereby. As a result, for example, where only the rolling code on the transmitter 1 is updated but the value of the rolling code restored from the transmission code falls within the permissible range and is determined as being normal, an error occurs between the rolling code set in the transmitter 1 and that set in the receiver 2. However, since in such a case the rolling code on the receiver 2 is updated by the rolling code restored from the transmission code, the rolling code on the transmitter 1 and that on the receiver 2 coincide with each other. Further, in step 170, the control objects 3-1, 3-2, ---, 3-n are operated in corresponding relation to the function bits (K1, K0) set in the transmission code via the drive circuits 23-1, 23-2, ---, 23-n. Although this embodiment has been directed to controlling several control objects, a transmission code with no function bit can also be realized by providing a single function as the function of the system.

[Second Embodiment]

This embodiment is directed to determining whether or not a transmission signal has continued to be transmitted for a prescribed time period (whether or not the switch has been continually depressed for the prescribed time period) and, where the transmission signal has continued to be transmitted for at least the prescribed time period, updating (reregistering) the bit-data rearranging order setting registered on the receiver side and to this end transmitting a new bit-data rearranging order setting from the transmitter 1 to the receiver 2.

The operations of the transmitter 1 and the receiver 2 will now be explained according to the flow chart illustrated in Figs. 6 and 7, in which the same reference numerals are used to denote the same or similar steps as in the first embodiment.

First, in step 10 through 70, the similar processes are performed as in the first embodiment. That is, it is determined whether or not any one of the switches has been depressed as in the first embodiment. Where the switch has been depressed, the rolling code is updated and an exclusive-OR operation is performed between the rolling code and the ID code. Then, the resulting code bit data items are rearranged according to a relevant bit-data rearranging order setting to thereby perform a transmission-code transmission processing. However, the operation of setting the bit-data rearranging order according to a 4-bit random number and the operation of adding this 4-bit random number to the transmission code are not included among the operations in steps 10 through 70.

Namely, if the switch has only been depressed, the bit-data rearranging order setting remains as it previously was and is not updated. Therefore, the bit-data rearranging operation is performed according to the same bit-data rearranging order setting as in the previous transmission. Therefore, with no 4-bit random number being added to the transmission code, the receiver 2 restores according to the previous bit-data rearranging order setting. Namely, data corresponding to this 4-bit random number need not be added to the transmission code. Accordingly, in usual uses (where the switch is continually depressed, for example, for only several seconds or so), it is impossible for unauthorized person to decode it merely by interception thereof because data corresponding to the bit-position rearranging order setting is not contained in the transmission code.

However, if only the above-described processing is performed, the bit-data rearranging order setting remains fixed. Accordingly, there is the possibility that it may be found through tens of interceptions that the bit-data rearranging order setting involves a certain standard or rule of regularity. This problem is settled by updating (reregistering) the bit-data rearranging order setting and varying such regularity.

Specifically, in step 80, where the transmission signal is continually transmitted for more than a prescribed

WAVELYNX EX. 1003, Pg. 1373
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

period (where the switch is continually depressed for, for example, the prescribed time period from step 10), the processes in steps 20 and 90 through 93 are executed to thereby set a new bit-data rearranging order, according to which the bit-data items are rearranged. A 4-bit random number (C3, C2, C1, C0) resulting from the setting of the new bit-data rearranging order is added to the transmission code, thereby updating the bit-data rearranging order setting. On the other hand, as illustrated in Fig. 7, in step 121, on the receiver side it is determined whether or not 4-bit information corresponding to the relevant bit-data rearranging order setting is added to the transmission code. If such 4-bit information is added, the bit-data rearranging order setting to which it is added is stored in the memory and the previously stored bit-data rearranging order setting is updated thereby in step 122. Then, code restoration is performed according to the thus-updated bit-data rearranging order setting in step 124. If the above-mentioned 4-bit information is not added, code restoration is performed in step 123 according to the previous bit-data rearranging order setting as stored in the memory, whereby the receiver 2 maintains a corresponding relation to the transmitter 1. When the receiver 2 has succeeded in updating, the receiver 2 may have a structure wherein it transmits to the transmitter 1 a signal indicating that the receiver 2 has succeeded in updating, or a structure wherein it informs the user that the receiver 2 has succeeded in updating.

As mentioned above, the second embodiment has a structure of determining whether or not the transmission signal has continued to be transmitted for the prescribed time period and, only when it has been continually transmitted for at least the prescribed time period, updating the bit-data rearranging order setting. As a consequence, it is possible for the user to freely change the bit-data rearranging order setting by appropriately altering the transmission time period. In addition, if the user once alters the transmission time period, any bit-data rearranging order is prevented from being added to the transmission code from the next time if the transmission time period is within the prescribed time period. For this reason, the transmission code has no information on the bit-data rearranging order, so that even when it is intercepted, decoding thereof is practically impossible.

Additionally, in the above-explained embodiment, where the transmitter 1 transmits the transmission code, a plurality of kinds of bit-data rearranging order settings each including prescribed codes are set for the prescribed bit-data rearranging order settings as illustrated in Fig. 4. For this reason, a code which indicates what kind of bit-data rearranging order has been set has to be added to the transmission code. However, if one kind of bit-data rearranging order is set and the value thereof is set to be fixed, it becomes unnecessary to add to the transmission code a code indicating what bit-data rearranging order pattern has been set, although difficulty in decoding by interception is somewhat decreased. This makes it possible to simplify the production of a transmission code. In addition, in this case, since it is not necessary to provide bit-position rearranging order settings in the memory, it is possible to decrease the amount of data stored in the memory.

On the other hand, in the above-mentioned embodiments, when exclusive-OR operation is performed, this operation is performed by setting the rolling code to a prescribed combination [6-bit fixed value (R1, R2, R1, R0, R0, R2)]. Therefore, the third embodiment illustrated in Fig. 8 may be also considered in which a plurality of combination patterns each including a prescribed code are set and, where the transmitter 1 transmits the transmission code, the transmitter 1 transmits this transmission code by adding to the transmission code a code which indicates according to what combination pattern the operation processing has been performed. By means of such embodiment, the code variation occurs in a more complex manner, thereby further increasing the difficulty in decoding by interception.

Further, in the above-mentioned embodiments, explanation has been given with respect to an ID code having a 6-bit configuration and with the rolling code having a 3-bit configuration. However, the present invention is not limited thereto but permits the number of the above-mentioned code bits to be set at any given value according to its purpose.

The present invention may be modified further in many other ways without departing from the spirit of the invention.

Claims

1. A remote control system comprising:

a transmitter (1) for transmitting a transmission code including an ID code prepared by encoding specific identifying information; and

a receiver (2) for receiving the transmission code transmitted from the transmitter, decoding the ID code and, where the ID code obtained by decoding thereof coincides with a preset ID code, outputting an instruction causing operation of a control object (3-1 through 3-n), wherein said transmitter (1) includes:

rolling code varying means (30) for, each time the transmitter transmits the transmission code, cumulatively varying a rolling code composed of a prescribed number of bits;

operation processing means (40) for performing an operation process with respect to each bit data item of the rolling code and each corresponding bit data item of the ID code, to vary each bit data item of the ID code in correspondence with the rolling code and thereby set a variable ID code,

bit-data rearranging means (50) for rearranging each bit data item of the variable ID code and each bit data item of the rolling code according to a prescribed bit-data rearrangement order setting; and

transmission code producing means (60, 70)

WAVELYNX EX. 1003, Pg. 1374
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

for producing a transmission code from a code having the bit data items rearranged by the bit-data rearranging means, and wherein said receiver (2) includes:

bit-data rearranging and restoring means (120) for, when receiving the transmission code from the transmitter, extracting the code having the rearranged bit data items and rearranging these rearranged bit data items according to the prescribed bit-data rearranging order setting to thereby restore the variable ID code and the rolling code;

operation processing and restoring means (130) for performing an inverse operation with respect to the restored variable ID code and the restored rolling code to thereby restore the ID code; and

comparing and determining means (140 - 170) for comparing the restored ID code and an ID code preset in the receiver and, when both ID codes coincide with each other, outputting a signal causing operation of the control object.

2. A remote control system as set forth in claim 1,

wherein the operation processing means (40) combines the bits of the rolling code by the same number as that of the bits of the ID code according to a prescribed combination setting and performs an exclusive-OR operation between each bit data item of the combined rolling code and each corresponding bit data item of the ID code to thereby set the variable ID code.

3. A remote control system as set forth in claim 1,

wherein the rolling code varying means (30) adds or subtracts a prescribed value to or from the rolling code each time the transmitter transmits the transmission code, to vary the rolling code in only one direction and thereby cumulatively vary the rolling code, and

wherein the comparing and determining means (140-170) further includes rolling code comparing and determining means (150) for comparing the rolling code restored by the operation processing and restoring means with the rolling code preset in the receiver and for, when a difference therebetween obtained by comparison is within a prescribed range, determining that the restored rolling code is correct.

4. A remote control system as set forth in claim 3,

wherein, where it has been determined by the rolling code comparing and determining means that the restored rolling code is correct, the restored rolling code is stored (160).

5. A remote control system as set forth in claim 1,

wherein a plurality of kinds of bit-data rearranging order settings each including prescribed codes are provided as the prescribed bit-data rearranging order settings and, when the transmitter transmits the transmission code, at least one kind is set from among the plurality of kinds of bit-data rearranging order settings, whereupon a rearranged code corresponding to said one kind of bit-data rearranging order setting is added (60) to the transmission code by the transmission code producing means.

6. A remote control system as set forth in claim 5,

wherein at least one kind is set from among the plurality of kinds of bit-data rearranging order settings by a random number.

7. A remote control system as set forth in claim 5,

wherein the transmitter (1) further includes:

transmission time period determining means (80) for determining whether or not a prescribed time period has passed from start of transmission;

the bit-data rearranging means (91) rearranges the bit data items according to the prescribed bit-data rearranging order setting as preset;

the transmission code producing means stopping the rearranged code from being added to the transmission code when it has been determined that the transmission time period is not longer than the prescribed time period;

the bit-data rearranging means updating the prescribed bit-data rearranging order setting and rearranging the bit data items according to the updated prescribed bit-data rearranging order setting; and

the transmission code producing means adding the rearranged code corresponding to the updated prescribed bit-data rearranging order setting to the transmission code when it has been determined that the transmission time period is longer than the prescribed time period, and

wherein the receiver (2) further includes:

rearranged code addition determining means (121) for, when receiving the transmission code from the transmitter, determining whether or not the rearranged code is added to the transmission code;

the bit-data rearranging and restoring means rearranging the bit data items according to the prescribed bit-data rearranging order setting corresponding to the rearranged code and storing this prescribed bit-data rearranging order setting when the rearranged code is added; and

the bit data items being rearranged according to the prescribed bit-data rearranging order setting as preset when the rearranged code is not added.

8. A method for a remote control system having a transmitter (1) for transmitting a transmission code including an ID code prepared by encoding specific identifying information and a receiver (2) for receiving the transmission code transmitted from the transmitter, decoding the ID code and, where the ID

WAVELYNX EX. 1003, Pg. 1375
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

code obtained by decoding thereof coincides with a preset ID code, outputting an instruction causing operation of a control object (3-1 through 3-n), said method comprising the steps of:

cumulatively varying (30) a rolling code composed of a prescribed number of bits, each time the transmitter transmits the transmission code;

performing (40) an operation process with respect to each bit data item of the rolling code and each corresponding bit data item of the ID code, to vary each bit data item of the ID code in correspondence with the rolling code and thereby set a variable ID code;

rearranging (50) each bit data item of the variable ID code and each bit data item of the rolling code according to a prescribed bit-data rearrangement order setting; and

producing (60, 70) a transmission code from a code having the bit data items rearranged by the bit-data rearranging step.

9. A method as set forth in claim 8, further comprising the steps of:

determining (80) whether or not a prescribed time period has passed from start of transmission;

rearranging (91) the bit data items according to the prescribed bit-data rearranging order setting as preset;

the rearranged code being stopped from being added to the transmission code when it has been determined that the transmission time period is not longer than the prescribed time period;

the prescribed bit-data rearranging order setting being updated and the bit data items being rearranged according to the updated prescribed bit-data rearranging order setting; and

the rearranged code corresponding to the updated prescribed bit-data rearranging order setting to the transmission code is added when it has been determined that the transmission time period is longer than the prescribed time period.

10. A method for a remote control system having a transmitter (1) for transmitting a transmission code including an ID code prepared by encoding specific identifying information and a receiver (2) for receiving the transmission code transmitted from the transmitter, decoding the ID code and, where the ID code obtained by decoding thereof coincides with a preset ID code, outputting an instruction causing operation of a control object (3-1 through 3-n), said method comprising the steps of:

extracting (120), when receiving the transmission code from the transmitter, the code having the rearranged bit data items and rearranging the rearranged bit data items according to the prescribed bit-data rearranging order setting to thereby restore the variable ID code and the rolling code;

performing (130) an inverse operation with respect to the restored variable ID code and the restored rolling code to thereby restore the ID code; and

comparing (140-170) the restored ID code and an ID code preset in the receiver and, when both ID codes coincide with each other, outputting a signal causing operation of the control object.

11. A method as set forth in claim 10, further comprising the steps of:

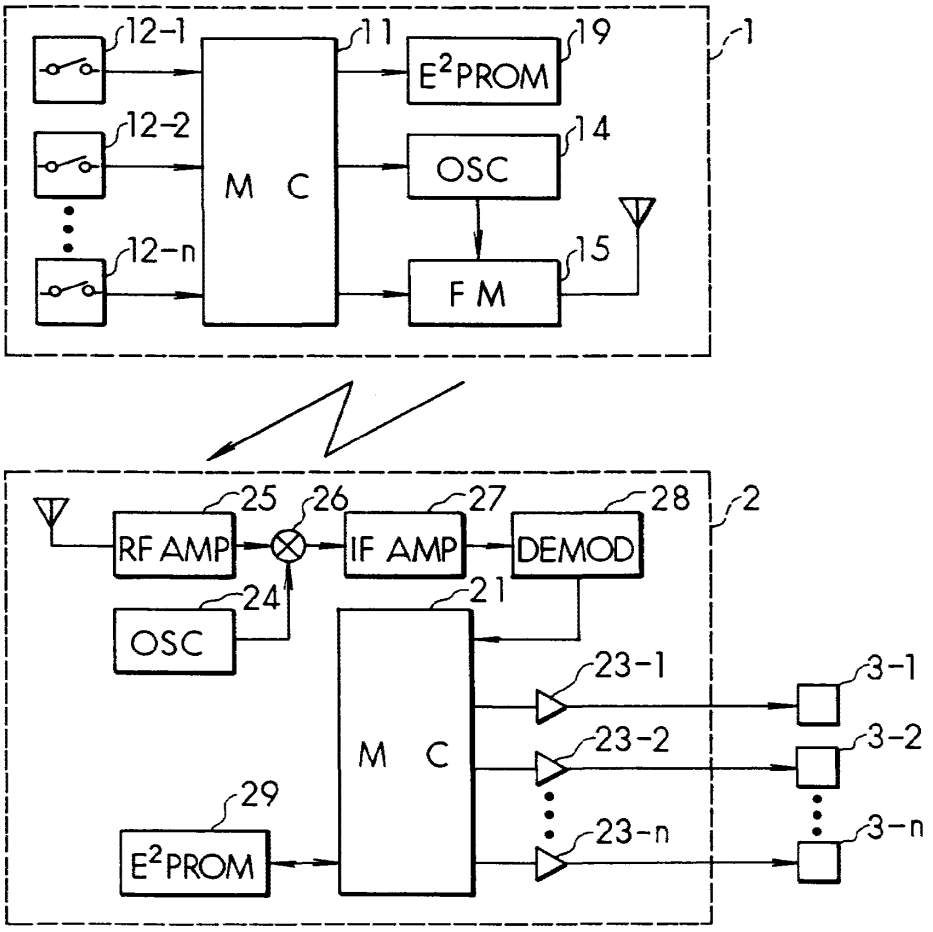
determining (121) whether or not the rearranged code is added to the transmission code, when receiving the transmission code from the transmitter;

the bit data items being rearranged according to the prescribed bit-data rearranging order setting corresponding to the rearranged code and the prescribed bit-data rearranging order setting being stored when the rearranged code is added; and

the bit data items being rearranged according to the prescribed bit-data rearranging order setting as preset when the rearranged code is not added.

WAVELYNX EX. 1003, Pg. 1376
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 1



WAVELYNX EX. 1003, Pg. 1377
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 2A

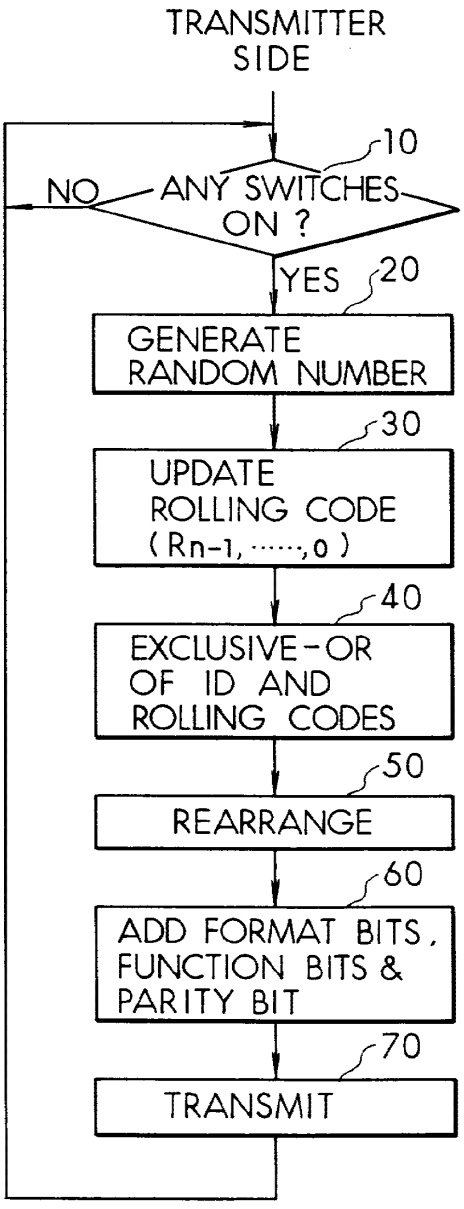
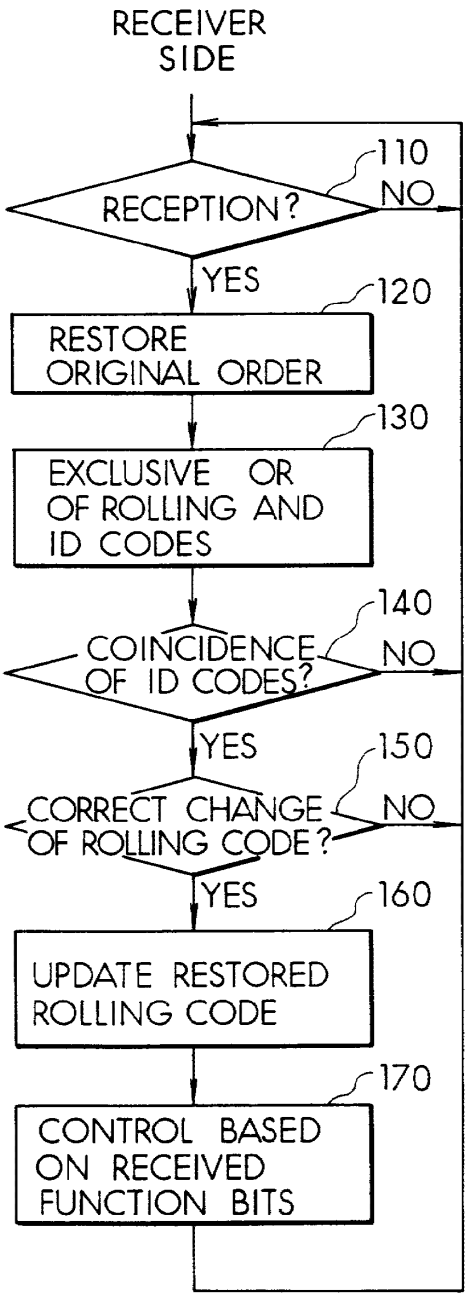
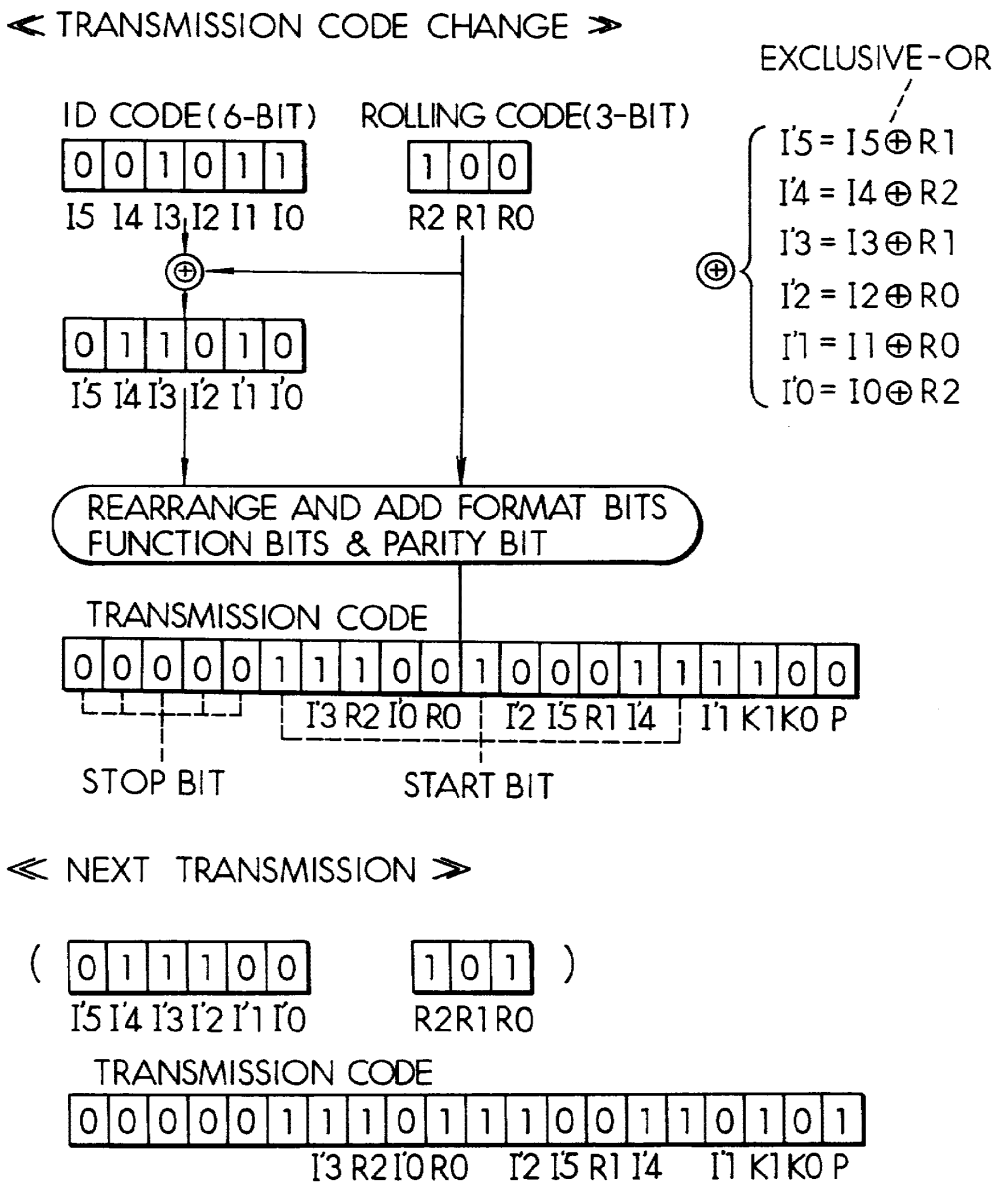


FIG. 2B



WAVELYNX EX. 1003, Pg. 1378
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 3



WAVELYNX EX. 1003, Pg. 1379
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

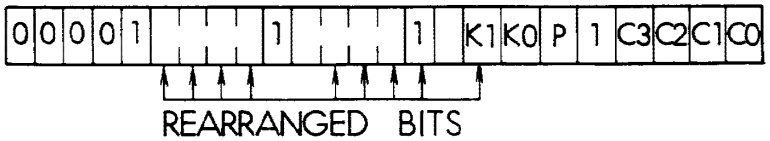
FIG. 4

EXAMPLE OF REARRANGEMENT PATTERN TABLE

(I'5 – I'0 AND R2 – R0 ARE REARRANGED)

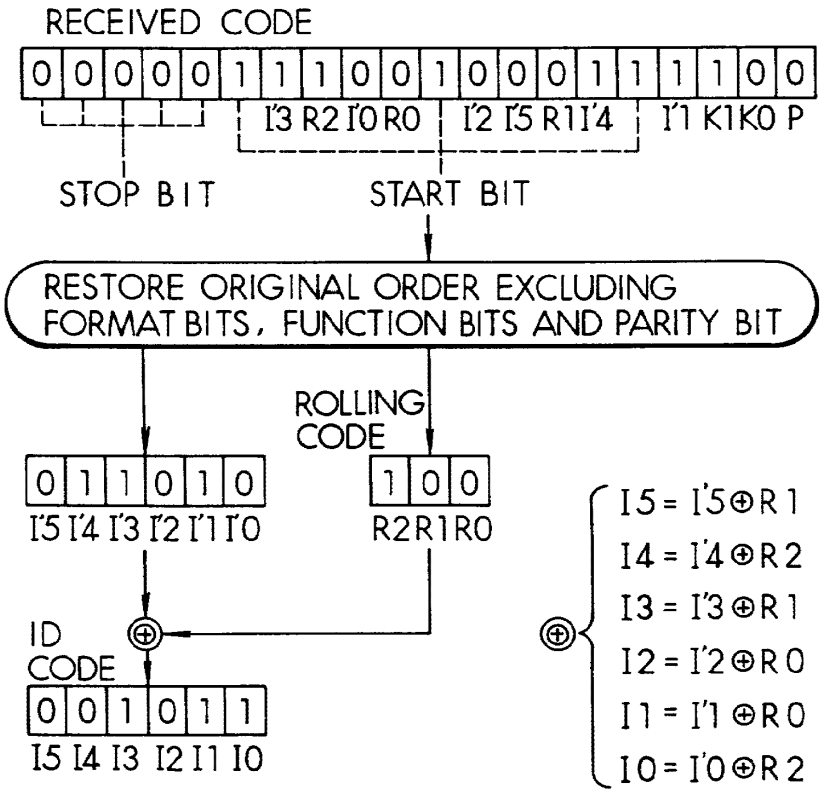
C3	C2	C1	C0	REARRANGING ORDER								
0	0	0	0	I'3	R2	I'0	R0	I'2	I'5	R1	I'4	I'1
			1	I'1	R0	I'5	I'3	R2	I'4	I'2	I'0	R1
		1	0	R2	I'0	I'2	I'4	R1	I'1	R0	I'3	I'5
			1	I'4	R1	I'1	I'0	R2	I'3	I'5	R0	I'2
	1	0	0	I'5	I'3	R0	I'2	I'4	R1	I'0	I'1	R2
			1	I'0	I'1	R2	I'5	I'3	R0	I'4	I'2	R1
		1	0	R1	I'2	I'4	R2	I'1	I'5	I'3	R0	I'0
			1	I'3	I'5	R2	R0	I'0	I'2	I'1	R1	I'4
1	0	0	0	I'1	R1	I'3	R2	I'5	I'0	I'4	R0	I'2
			1	I'2	I'4	R1	I'1	R0	I'3	R2	I'5	I'0
		1	0	R0	I'0	R2	I'3	R1	I'1	I'5	I'2	I'4
			1	I'4	I'5	I'2	R1	I'0	R0	I'3	R2	I'1
	1	0	0	I'2	R0	I'3	R2	I'1	I'4	R1	I'0	I'5
			1	R0	R2	I'1	I'4	I'5	I'0	I'2	R1	I'3
		1	0	I'5	I'2	I'0	I'1	I'4	R0	R2	I'3	I'1
			1	I'0	I'3	I'4	R0	I'2	R2	R1	I'1	I'5

TRANSMISSION CODE INCLUDING C3 – C1



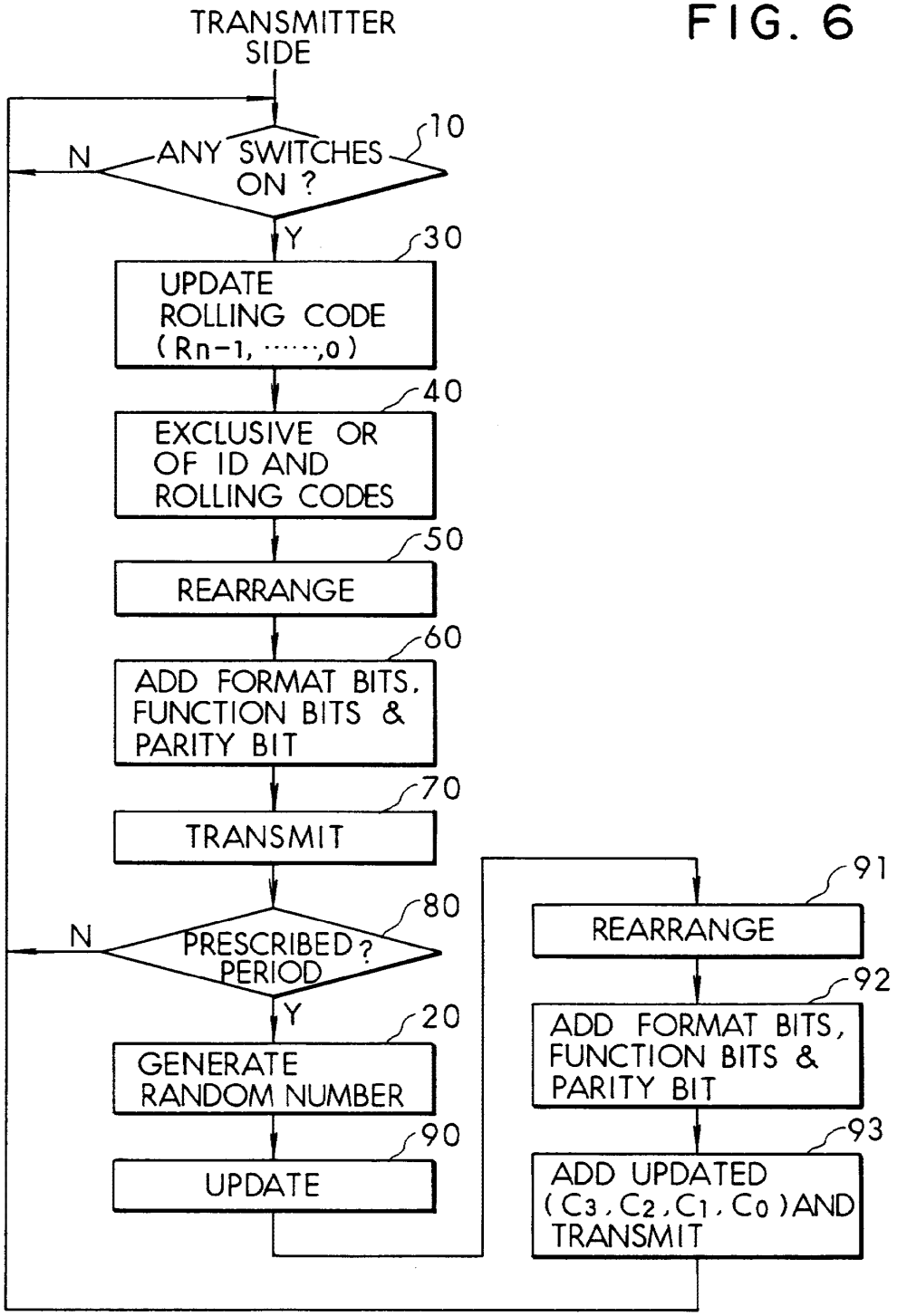
WAVELYNX EX. 1003, Pg. 1380
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 5



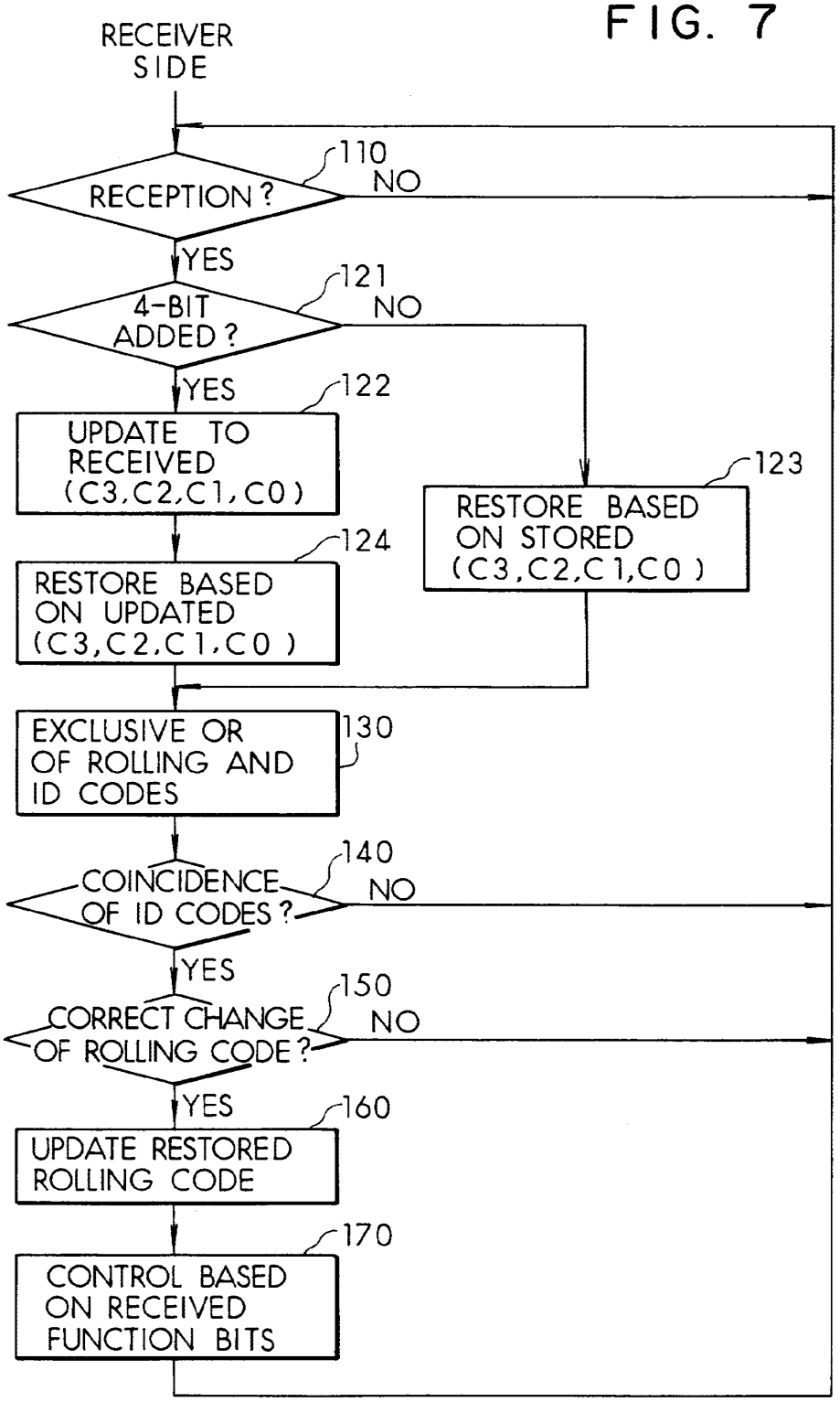
WAVELYNX EX. 1003, Pg. 1381
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 6



WAVELYNX EX. 1003, Pg. 1382
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 7



WAVELYNX EX. 1003, Pg. 1383
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 8

EXAMPLE OF COMBINATION PATTERN TABLE
(R2-R0 ARE COMBINED WITH I5-I0)

CODE				COMBINATION					
D3	D2	D1	D0	I5	I4	I3	I2	I1	I0
0	0	0	0	R2	R2	R1	R1	R0	R0
			1	R2	R2	R1	R0	R0	R1
		1	0	R2	R2	R0	R1	R0	R1
			1	R2	R2	R1	R0	R1	R0
	1	0	0	R0	R0	R1	R2	R1	R2
			1	R1	R2	R0	R0	R2	R1
		1	0	R2	R2	R0	R0	R1	R1
			1	R1	R0	R2	R0	R2	R1
1	0	0	0	R0	R2	R1	R0	R2	R1
			1	R2	R2	R0	R1	R1	R0
		1	0	R0	R1	R2	R0	R2	R1
			1	R1	R0	R0	R2	R1	R2
	1	0	0	R0	R0	R2	R1	R2	R1
			1	R1	R0	R1	R0	R2	R2
		1	0	R0	R1	R0	R2	R1	R2
			1	R1	R2	R1	R0	R0	R2

TRANSMISSION CODE INCLUDING D3-D0

0	0	0	0	0	1	I'3	R2	I'0	R0	1	I'2	I'5	R1	I'4	1	I'1	K1	K0	P	1	D3	D2	D1	D0

WAVELYNX EX. 1003, Pg. 1384
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 11 2156

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	GB-A-2 265 482 (TIBBETTS) * page 5, line 8 - page 11, line 1; figure 1 * ---	1,3,8	E05B49/00
A	EP-A-0 570 761 (LECTRON PRODUCTS,INC.) * page 8, line 16 - page 9, line 14; figure 9 * ---	1,2,8,10	
P,A	WO-A-94 18036 (ROBERT BOSCH GMBH) * page 4, line 17 - page 7, line 15; figures 1,2 * -----	1-3,8,10	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)
			E05B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	25 October 1995	Herbelet, J.C.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1385
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 October 2002 (17.10.2002)

PCT

(10) International Publication Number
WO 02/082367 A1

(51) International Patent Classification[7]: G06K 19/06, 7/10

(21) International Application Number: PCT/US02/10554

(22) International Filing Date: 6 April 2002 (06.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/828,395 6 April 2001 (06.04.2001) US

(71) Applicant *(for all designated States except US)*: **PITTWAY CORPORATION** [US/US]; 200 South Wacker Drive, Suite 700, Chicago, IL 60606 (US).

(71) Applicants and
(72) Inventors: **DAVIS, Michael** [US/US]; 12 Hummingbird Lane, Amherst, NY 14228 (US). **HULUSI, Tam** [US/US]; 16 Harborview Drive, Northport, NY 11768 (US).

(74) Agent: **BARKUME, Anthony, R.**; 20 Gateway Lane, Manorville, NY 11949 (US).

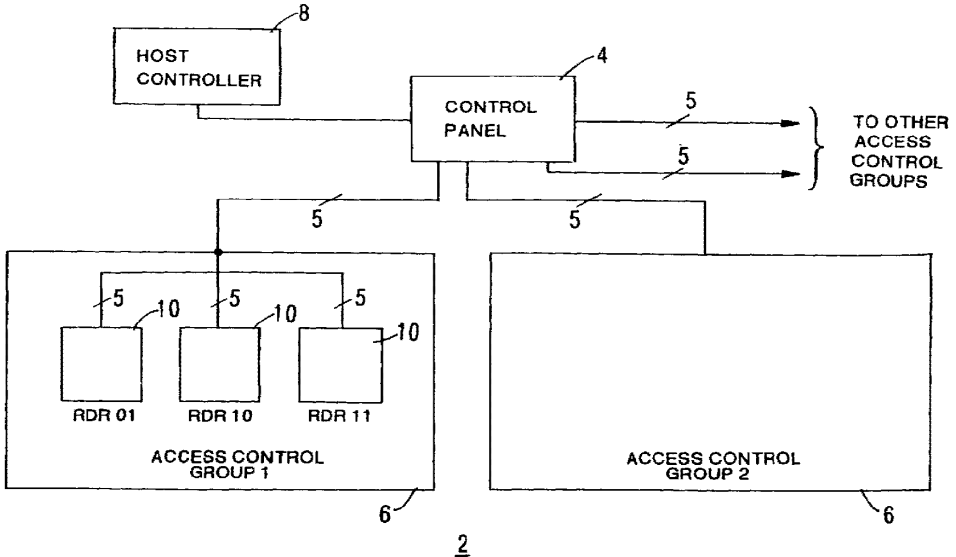
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CO, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: SYSTEM AND METHOD OF EXTENDING COMMUNICATIONS WITH THE WIEGAND PROTOCOL



2

(57) Abstract: An extension of the industry standard Wiegand protocol (2) for enabling two way extended communication, enhanced error detection, encryption, multiple reader capability, and enhanced information regarding the embedded data stream between a Wiegang device such as a card reader (10) and a control panel (4) on the existing 5-wire bus structure without requiring the modification to the existing infrastructure.

WO 02/082367 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD OF EXTENDING COMMUNICATIONS WITH THE WEIGAND PROTOCOL

TECHNICAL FIELD

This application relates to access control systems, and in particular to a system and method for utilizing an existing Wiegand infrastructure to support readers and panels with extended data communications functionality.

BACKGROUND ART

Access control systems are used for controlling automated access to protected premises, typically through doorways, without requiring in-person security personnel. Typically, a device such as a card reader is positioned near a doorway of a secure area such as a computer room. A person desiring to enter the secure area must present to the reader a card having user data that can be read by the reader. The reader will transmit the user data via a hardwired bus to a control system typically consisting of numerous control panels ultimately connected back to a host computer, which will decide based on certain rules if that person should be allowed to enter the premises at that door. For example, the host computer may be programmed to let certain users in at only certain times of the day, such as normal working hours, or it may be programmed to allow certain users in at all times, or it may be programmed to disallow entry to certain users. If the host computer determines that access should be allowed, it will send a command that will, for example, activate a relay that will open a door strike mechanism, thusly allowing entry by the user that presented the card.

WAVELYNX EX. 1003, Pg. 1388
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

One technology in prevalent use for many years is the Wiegand protocol, which utilizes five wires to communicate data and provide power to a dedicated card reader as well known in the art. The five wires are for power, ground, DATA0, DATA1, and LEDCTL. The DATA1 line is a reader output that delivers pulses that are interpreted as binary ones. The DATA0 line is a reader output that delivers pulses that are interpreted as binary zeros. The LEDCTL line is the panel output that determines the state of the LED contained on the reader (off, red, green, or amber). The Wiegand standard protocol well known in the art and is described in detail in "Access Control Standard Protocol for the 26-Bit Wiegand Reader Interface," by the Security Industry Association. The data bits of the transmission from the reader to the panel typically consists of one or more parity bits and numerous data bits, as described in the aforementioned standard. The definition of the data bits are left to the system designer. For example, one data format uses the first 8 bits as a site code (0-255), and the next 16 bits as the card number (0-65,535).

Certain problems exist with the Wiegand protocol, however. For example, the Wiegand protocol is a one-way protocol, since the reader can send data to the panel but the panel cannot send any data to the reader except to control the door mechanism and a status LED. The ability to detect errors is weak because most Wiegand formats only include a leading and trailing parity bit, and wire runs up to 500 feet in an electrically noisy area enhances the possibility of a data transmission error. Further, if the panel detects a data transmission error, there is no way at the present time for it to signal the error detection back to the reader (to obtain a retransmission). The reader has no method of signaling additional information except the

WAVELYNX EX. 1003, Pg. 1389
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ability to control the reader LED. Moreover, there is no way to attach multiple Wiegand readers in a party-line connection scheme and determine which reader generated the data. Finally, there exists no security (such as encryption) between the reader and the panel.

It is therefore an object of the invention to provide a methodology and system for extending the functionality of the Wiegand protocol such that improved readers and panels may be implemented, without requiring rewiring of the existing Wiegand infrastructure in use today.

It is a further object of the invention to provide such a methodology and system for extending the Wiegand protocol while still allowing prior art Wiegand readers to communicate with the panel, such that existing system can be upgraded with certain readers while still allowing existing readers to function in their original manner.

It is a further object of the invention to provide such a methodology and system for extending the Wiegand protocol that will allow improved functionality in the reader such that the user can provide different types of data inputs to the panel.

DISCLOSURE OF THE INVENTION

Thus, provided is an improvement on the existing Wiegand system, wherein the first major difference is that additional bits are appended to the data stream, which provide supplementary information from the reader (which may or may not be related to a card read) as well as a CRC or other type of error detection and/or correction bits covering all of the data in the transmission. A second

WAVELYNX EX. 1003, Pg. 1390
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

major improvement is that the LEDCTL line controlled by the panel is now used to transmit data back to the reader.

As a result of this invention, described herein, no additional wires are required to be connected between the panel and the reader, thus preserving the existing Wiegand infrastructure while providing increased functionality. The panel computer will require no changes to its interface (or other) hardware; only the firmware needs to be modified in accordance with the invention. Messages can be customized by users in accordance with the extended protocol set forth herein.

The Wiegand extension can be turned on or off, so that if a panel does not support the extension, it is not used and the reader behaves as an existing prior art device.

Thus, in accordance with the present invention, provided is an access control security system including a control panel and a plurality of access control groups. Each access control group is interconnected to the control panel on an independent multi-wire Wiegand data bus. Each access control group includes at least one access interface unit that has data output means for transmitting data onto the data bus to the control panel, data input means for receiving data via the data bus from the control panel, and processing means. The processing means interoperates with the data output means and the data input means, and operates data transfers over the data bus. In particular, the processing means is adapted to generate a data message for transmission onto the data bus via the data output means, wherein the data message has a Wiegand message field in accordance with the existing Wiegand protocol, as well as an extended data field. The extended data field can include a

WAVELYNX EX. 1003, Pg. 1391
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

status information field indicative of a status condition of the access interface unit. Data transfers are made to the control panel using the electrical and information content of the Wiegand protocol via the Data "0" and Data "1" output signals. Data transfers are made by the control panel using the electrical characteristics of the Wiegand protocol via the LEDCTL input signal as a serial protocol.

The access interface unit further includes user ID reading means for reading an ID device. For example, the ID reading means may be configured to read an access control card, a data transponder, a data-carrying key fob, or biometric data from a user. The processing means interoperates with the ID reading means, and the extended data field includes an information field indicative of a property of an ID read by the ID reading means.

In the system of the present invention, an access control group may include more than one access interface units, in which case the extended data field then includes address information uniquely identifying each access interface unit in an access control group.

The processing means may be adapted to utilize an error detection algorithm such as a CRC as a function of data contained within the extended data field.

The access interface unit may further include user input means (such as pushbutton) for accepting user input functions (such as a door bell), and the status condition of the access interface unit may indicate a function input by a user via the user input means.

WAVELYNX EX. 1003, Pg. 1392
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

The access interface unit may also include external status input means for accepting external status data from an external device coupled thereto, and the status information field of the extended data field then will include the external status data. For example, the external device may be adapted to measure temperature, in which case the external status data is the measured temperature. The external device may also be adapted to detect a change in light incident thereon, or it may be adapted to detect physical tampering with the access interface unit.

The processing means may be further adapted to generate supervision data on a periodic basis, and the status information field could then include the supervision data.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is a block diagram of the system of the preferred embodiment.

Fig. 2 is an illustration of the extended Wiegand data protocol of the present invention.

Fig. 3 is a block diagram of the Wiegand reader of the preferred embodiment.

BEST MODE FOR CARRYING OUT THE INVENTION

Figure 1 illustrates a system block diagram of the preferred embodiment of the present invention. The access control system 2 includes a control panel 4 which is used to communicate via several 5-wire buses to various access control groups 6. A host controller 8 provides master data processing and control for one or more control panels 4 as illustrated. Thus, depending on the topology and layout of a building or campus under control, the system 2 can be

WAVELYNX EX. 1003, Pg. 1393
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

adapted via various combinations of control panels 4 and access control groups 6.

Each access control group 6 contains up to three access interface units (card readers) 10, as shown in access control group 1 in Figure 1. Since two address bits are used in the extended protocol described herein, four different addresses are possible. Address 00 is reserved for a broadcast message in the preferred embodiment, so addresses 01, 10 and 11 are useable for discrete readers 10. In the prior art, each 5-wire bus could only communicate with one such card reader 10 since addressing was not possible under the standard Wiegand protocol. Multiple card readers tied to the same 5-wire bus are useful, for example, in situations where it is desired to place one reader on one side of a door and another reader on the other side of the door, thus controlling access in both directions with the same 5-wire interface.

A block diagram of each access interface unit (card reader) 10 is shown in Figure 3. A Wiegand transmitter 12, Wiegand receiver 14, and power supply circuit 16 are all shown; these operate functionally the same as in prior art Wiegand devices well known in the art. The transmitter 12 and receiver 14 are connected to the DATA1, DATA0, and LEDCTL wires of the standard Wiegand interface as known in the art. Also shown in Figure 3 is an RF transmitter/receiver 26, which is known in the art and which is used for reading an access control card when presented thereto.

A tamper and temperature sensing interface 18 is shown in Figure 3, which allows connection of the reader 10 to external tamper and temperature sensing devices. By

WAVELYNX EX. 1003, Pg. 1394
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

using a temperature sensor, temperature data may be transmitted back to the control panel 4 with the extended data field. Likewise, by using a tamper sensor, an alarm may be sent to the control panel in the event that someone attempts to alter or destroy the reader 10, and such activity is sensed by the tamper sensor. These types of sensors are well known in the art and need not be described in detail herein.

Also provided is a button/switch interface 20, which is connected to one or more buttons and/or switches that may reside on the housing of the reader 10. These buttons can be programmed to indicate virtually anything that may be desired by the system designer; for example a doorbell function described further below is easily attained by using a doorbell button with the extended protocol. This allows a person without an access card (e.g. a building visitor) to signal that he desires attention at the reader 10 by simply pressing the doorbell button. The doorbell status would be transmitted to the control panel without requiring the use of additional wires as in the prior art.

Also shown in Figure 3 is LED control block 22, which is used to drive one or more LEDs associated with the reader 10. While the prior art Wiegand systems relied on the LEDCTL wire for this function, the extended protocol allows more data to be communicated to the reader 10, thus providing more sophisticated LED (or other) outputs as desired.

Processor 24 is used to read data from the external sources, formulate data to be transferred over the 5-wire interface, and run all other functions that may be required by the reader 10 of the present invention.

WAVELYNX EX. 1003, Pg. 1395
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

In the preferred embodiment, the extended Wiegand protocol adds an additional 18 bits to the prior art (basic) Wiegand data transmission, although of course any amount of extension bits could be added as desired. The first two bits are used for address data to determine which Wiegand reader (also referred to as a Wiegand generator or an access interface unit) generated the data in a party-line configuration in a given access control group, where there is more than one reader available for communications. The next 8 bits contain an information field (message number), and the last eight bits contain a CRC of all preceding bits including the basic Wiegand data. If the panel determines that there is an error in the received Wiegand data (i.e. due to a CRC error), then it can request the reader to retransmit as described herein. The extended protocol is shown in Figure 2.

The address field (first two bits) is used to distinguish among multiple Wiegand readers sharing the same Wiegand 5-wire bus. In the preferred embodiment, address 00 is reserved for broadcast messages, and addresses 01, 10, and 11 are used to distinguish among multiple readers. An address of 00 is the default when multiple-unit addressing is not used.

Since the electrical characteristics of the Wiegand interface call for open-collector drivers, multiple readers can be attached to the same Wiegand bus. Note that with the robust error checking enabled by the present invention, any attempt by multiple Wiegand generators to talk at the same time (so-called "collisions") will be detected, and then the panel will send out a "rebroadcast

WAVELYNX EX. 1003, Pg. 1396
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

message" request using either address 00 or one-by-one to each of the active generators.

In the preferred embodiment, there are seven groups of messages; each is used for different Wiegand generators. For example, these categories include security/access control, time & attendance, parking, etc. Group zero is reserved for messages common to all group, and group 7 is reserved for error messages.

Data transfer from panel to reader

In accordance with the invention, the panel may send data to a reader using an asynchronous serial data stream via the LEDCTL wire at 1200 baud, 8 data bits, 1 stop bit, no parity. All fields in this instance are one byte long. The first byte of a command is divided into two sub-fields. The first two bits are the address field (00-11), and the last six bits contain the command code (000000-111111). The following commands are available in the preferred embodiment:

COMMAND SENT BY PANEL		WIEGAND GENERATOR RESPONSE
00h <CRC>	0 = retransmit last Wiegand data transmission <CRC> = 8-bit CRC	Retransmits last Wiegand data message
01h <address> <CRC>	1=Return value of selected parameter address <address> = 00 thru FF <CRC> = 8-bit CRC	Parameter value of desired address is transmitted back via the Wiegand extension
02h <address> <data> <CRC>	2= set value of selected parameter address <address> = 00 thru FF <data> = 00 thru FF <CRC> = 8-bit CRC	Acknowledgement that data was written is transmitted via the Wiegand extension
03h <LEDCTL> <seconds> <CRC>	3=Turn on LED <LEDCTL> = simulation of LED control signals <# of seconds to keep LED on> <CRC> = 8-bit CRC	Acknowledgement is transmitted via the Wiegand extension

WAVELYNX EX. 1003, Pg. 1397
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

The panel system in the preferred embodiment is able to switch a Wiegand generator from the basic protocol to the extended protocol as follows. Note that this procedure will typically be run when the panel is initialized. The panel will drop the LEDCTL signal low three times within a one-second interval. The Wiegand generator starts an interval timer when the first pulse is received, and then checks to see if it receives two additional pulses within the one-second period from the first pulse. If it receives exactly three pulses as described, then it sends the Wiegand extension message "Capable of Using the Wiegand Extension" in message group 0. The panel then will send out the "Use Wiegand Extension" command to the Wiegand generator, and the Wiegand generator sends the "Command received and executed" message in group 0 and sets a flag in non-volatile memory to use the Wiegand extension (even if power is lost and subsequently restored).

Pushbutton Emulation

In another aspect of the invention, the reader includes one or more push buttons or other types of input devices on the housing that can be used to provide additional information to the panel. Rather than utilize separately added wires for pushbutton functions as in the prior art, this invention utilizes the Wiegand extension protocol to transmit the button data to the panel. Moreover, in this invention, buttons can be required to be pressed before a card will be accepted; button status is reported along with card data in the same Wiegand extension transmission, multiple buttons can be pressed to signify different functions, and buttons may have changeable legends

WAVELYNX EX. 1003, Pg. 1398
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

on the housing (since their functionality is easily reprogrammed).

Since the status of the buttons on the housing is reported using the extended Wiegand protocol described herein, no additional wires are required to be added to existing 5-wire Wiegand infrastructure.

A reader can be programmed to report the status of a button without requiring a card to be read. For example, a doorbell function may be emulated in this way, so that a visitor can press the button, causing a doorbell message to be sent to the panel. This can then alert a security person in the area that a visitor who does not have a card needs attention at that entry point. This eliminates the need to provide a separate, dedicated doorbell wiring system as in the prior art.

In addition, the arming and disarming functions of the related security system can now be easily implemented. That is, a user can arm or disarm the security system upon presentation of a valid card authorized for that function.

Similarly, legends such R and C can be used with separate buttons that would be pressed by a user leaving or entering a facility, who would then present the card for identification purposes. This enables the system to keep track of who is in the building at any given time.

A duress or panic condition could be used for example if a person presses a certain combination of buttons upon presentment of the card for entry.

WAVELYNX EX. 1003, Pg. 1399
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Panel operating parameters can be modified by button presses along with presentment of an authorized card.

CRC

The CRC field contains an 8-bit CRC of all of the preceding Wiegand data and the extended data field. CRC technology is well known in the art and need not be repeated herein.

WAVELYNX EX. 1003, Pg. 1400
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

We claim:

1. An access control security system comprising:
   a) a control panel;
   b) a plurality of access control groups, each access control group interconnected to the control panel on an independent multi-wire data bus, each access control group comprising:
      an access interface unit comprising:
         data output means for transmitting data onto the data bus to the control panel,
         data input means for receiving data via the data bus from the control panel,
         processing means, interoperating with the data output means and the data input means, for operating data transfers over the data bus, the processing means adapted to generate a data message for transmission onto the data bus via the data output means, the data message comprising a Wiegand message field in accordance with the Wiegand protocol and an extended data field.

2. The system of claim 1 wherein the extended data field comprises a status information field indicative of a status condition of the access interface unit.

3. The system of claim 1 wherein the access interface unit further comprises user ID reading means for reading an ID device.

WAVELYNX EX. 1003, Pg. 1401
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

4. The system of claim 3 wherein the ID reading means is configured to read an access control card.

5. The system of claim 3 wherein the ID reading means is configured to read a data transponder.

6. The system of claim 3 wherein the ID reading means is configured to read a data-carrying key fob.

7. The system of claim 3 wherein the ID reading means is configured to read biometric data from a user.

8. The system of claim 3 wherein the processing means interoperates with the ID reading means, and wherein the extended data field further comprises an information field indicative of a property of an ID read by the ID reading means.

9. The system of claim 1 wherein at least one access control group comprises a plurality of access interface units, and wherein the extended data field comprises address information uniquely identifying each access interface unit in an access control group.

10. The system of claim 1 wherein the processing means is further adapted to utilize an error detection algorithm as a function of data contained within the extended data field.

11. The system of claim 10 wherein the error detection algorithm is a cyclic redundancy check (CRC), and wherein the extended data field is appended with the CRC.

12. The system of claim 2 wherein the access interface unit further comprises user input means for accepting user input

WAVELYNX EX. 1003, Pg. 1402
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

functions, and wherein the status condition of the access interface unit indicates a function input by a user via the user input means.

13. The system of claim 12 wherein the input means comprises at least one pushbutton.

14. The system of claim 13 wherein the function of the pushbutton is a door bell function.

15. The system of claim 2 wherein the access interface unit comprises external status input means for accepting external status data from an external device coupled thereto, and wherein the status information field of the extended data field comprises the external status data.

16. The system of claim 15 wherein the external device is adapted to measure temperature, and wherein the external status data comprises the measured temperature.

17. The system of claim 15 wherein the external device is adapted to detect a change in light incident thereon, and wherein the external status data comprises data indicative of a change in light.

18. The system of claim 15 wherein the external device is adapted to detect physical tampering with the access interface unit, and wherein the external status data comprises a tamper indication.

19. The system of claim 2 wherein the processing means is further adapted to generate supervision data on a periodic basis, and wherein the status information field comprises the supervision data.

WAVELYNX EX. 1003, Pg. 1403
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

20. The system of claim 2 wherein the processing means is further adapted to detect a malfunction of the access interface unit, and wherein the status information field comprises data indicative of a malfunction.

21. The system of claim 1 wherein data transfers are made to the control panel using the electrical and information content of the Wiegand protocol via the Data "0" and Data "1" output signals.

22. The system of claim 1 wherein data transfers are made by the control panel using the electrical characteristics of the Wiegand protocol via the LEDCTL input signal as a serial protocol.

WAVELYNX EX. 1003, Pg. 1404
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

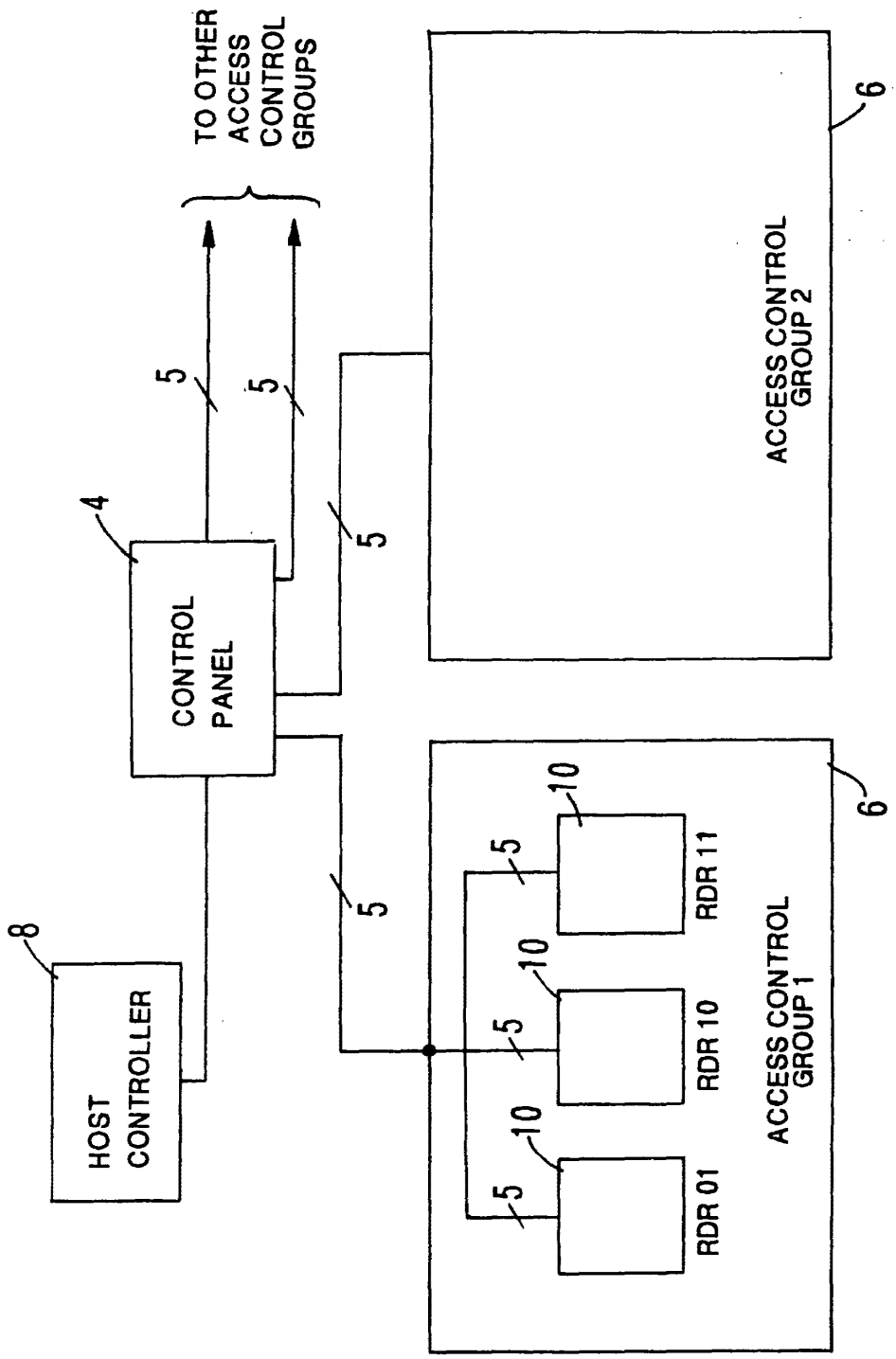

TO OTHER ACCESS CONTROL GROUPS
5
5
4
CONTROL PANEL
5
ACCESS CONTROL GROUP 2
6
5
10
RDR 11
5
10
RDR 10
5
10
RDR 01
5
ACCESS CONTROL GROUP 1
6
8
HOST CONTROLLER
2

FIG.1

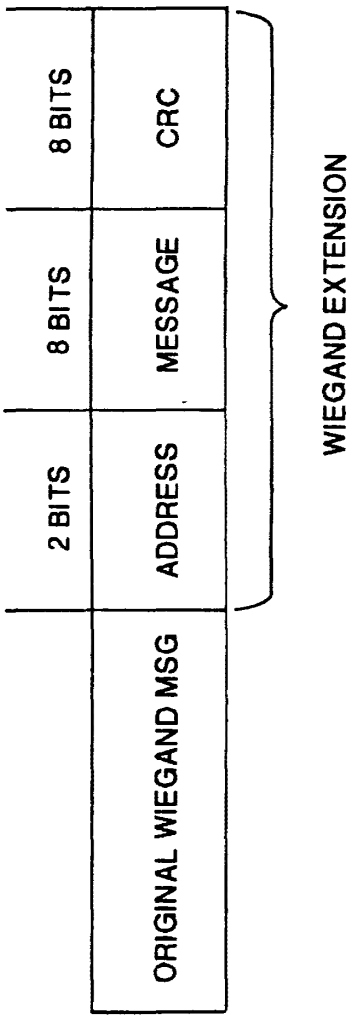

2 BITS
8 BITS
8 BITS
ADDRESS
MESSAGE
CRC
WIEGAND EXTENSION
ORIGINAL WIEGAND MSG

FIG.2

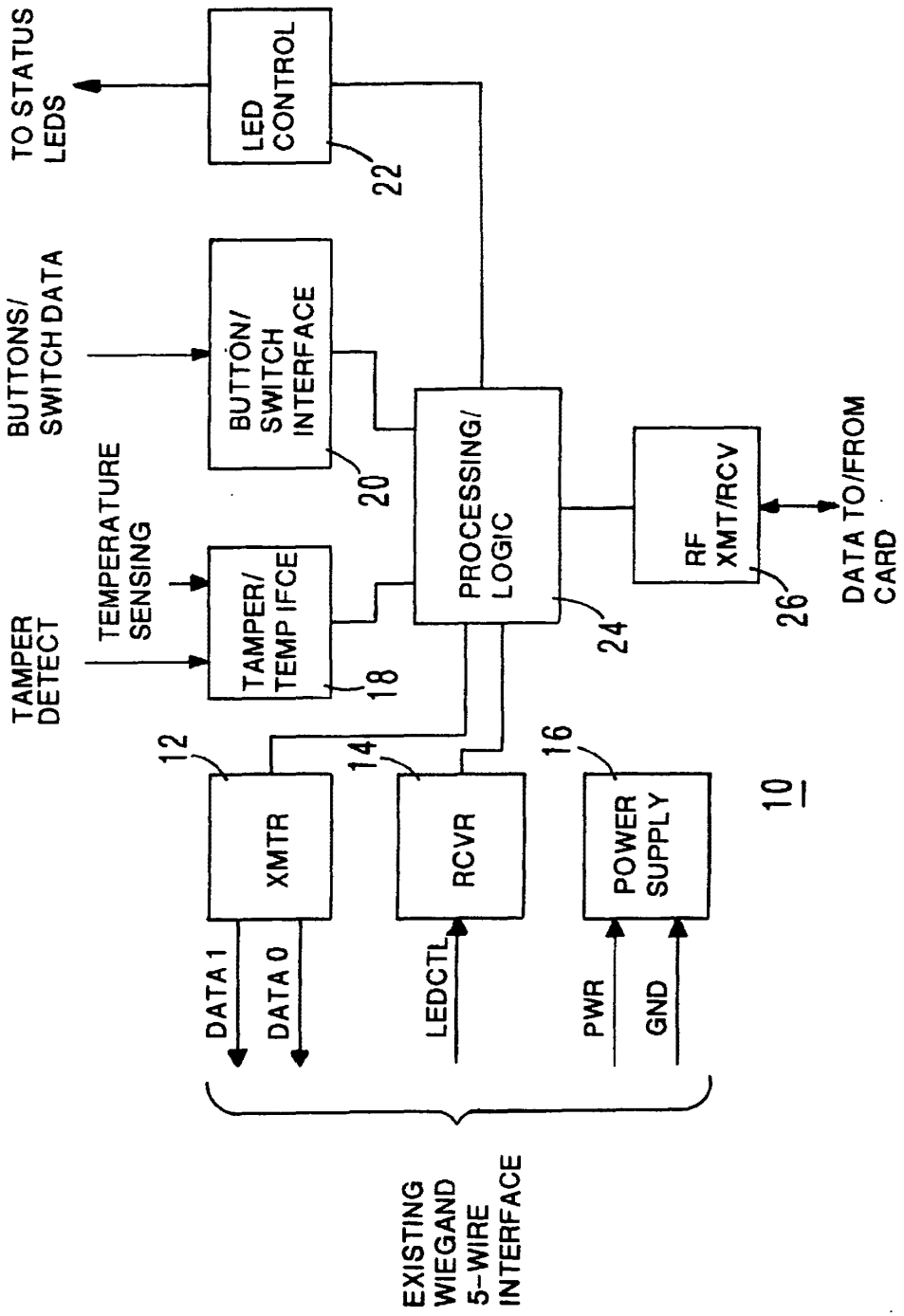

TO STATUS LEDS
LED CONTROL
22
BUTTONS/ SWITCH DATA
BUTTON/ SWITCH INTERFACE
20
TEMPERATURE SENSING
TAMPER DETECT
TAMPER/ TEMP IFCE
18
PROCESSING/ LOGIC
24
RF XMT/RCV
26
DATA TO/FROM CARD
12
XMTR
14
RCVR
16
POWER SUPPLY
10
DATA 1
DATA 0
LEDCTL
PWR
GND
EXISTING WIEGAND 5-WIRE INTERFACE

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/10554

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06K 19/06, 7/10
US CL : 235/ 381, 382, 382.5, 492, 486, 441, 375, 380, 384; 705/13, 41, 43, 44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 235/ 381, 382, 382.5, 492, 486, 441, 375, 380, 384; 705/13, 41, 43, 44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,517,172 A (CHIU) 14 May 1996 (05.14.1996), the entire document.	1-22
Y	US 5,491,471 A (STOBBE) 13 February 1996 (13.02.1996), the entire document.	1-22
A	US 5,166,676 A (MILHEISER) 24 November 1992 (24.11.1992), the entire document.	1-22
A	US 5,028,918 A (GILES et al) 02 July 1991 (02.07.1991), the entire document.	1-22
Y,E	US 6,411,199 B1 (GEISZLER et al) 25 June 2002 (25.06.2002), the entire document.	1-22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 July 2002 (24.07.2002)	05 SEP 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Le, Thien M. Telephone No. (703) 308-0956

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/10554

Continuation of B. FIELDS SEARCHED Item 3:
USPTO APS EAST
search terms: Wiegand, protocol, card$1, reader$1, two-way$1, 5-wire$2 bus$3, interface, panel

WAVELYNX EX. 1003, Pg. 1409
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 April 2008 (17.04.2008)

PCT

(10) International Publication Number
WO 2008/043125 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/AU2007/000311

(22) International Filing Date: 13 March 2007 (13.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2006905707 13 October 2006 (13.10.2006) AU

(71) Applicant *(for all designated States except US)*: **MICRO-LATCH PTY LTD** [AU/AU]; Unit 13, 145-147 Forest Road, Hurstville, NSW 2220 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **BROWN, Perry, Andrew** [AU/AU]; 67 Bredon Avenue, West Pennant Hills, NSW 2125 (AU).

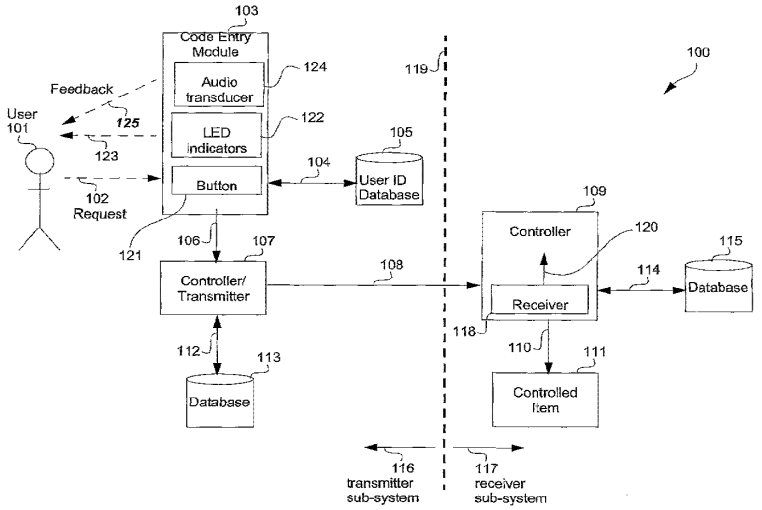
(74) Agent: **SPRUSON & FERGUSON**; GPO Box 3898, Sydney, NSW 2001 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) Title: A SECURE WIRELESS REMOTE ENTRY SYSTEM



(57) Abstract: A system (100) for providing secure access to a controlled item (111) is disclosed. The system (100) comprises a transmitter subsystem (116) comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, upon receiving the request, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier. The system (100) also comprises a receiver sub-system (117) comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item (111) dependent upon the code and the Wiegand protocol identifier.

WO 2008/043125 A1

A SECURE WIRELESS REMOTE ENTRY SYSTEM

Field of the Invention

The present invention relates to secure access systems and, in particular, to systems using wireless transmission of security code information.

Background

Fig. 1 shows a prior art arrangement for providing secure access. A user 401 makes a request, as depicted by an arrow 402, directed to a code entry module 403. The module 403 is typically mounted on the external jamb of a secure door. The request 402 is typically a secure code of some type which is compatible with the code entry module 403. Thus, for example, the request 402 can be a sequence of secret numbers directed to a keypad 403. Alternately, the request 402 may be a biometric signal from the user 401 directed to a corresponding biometric sensor 403. One example of a biometric signal is a fingerprint. Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, palm configuration and so on.

The code entry module 403 conveys the request 402 by sending a corresponding signal, as depicted by an arrow 404, to a controller 405 which is typically situated in a remote or inaccessible place. The controller 405 authenticates the security information provided by the user 401 by interrogating a database 407 as depicted by an arrow 406. If the user 401 is authenticated, and has the appropriate access privileges, then the controller 405 sends an access signal, as depicted by an arrow 408, to a device 409 in order to provide the desired access. The device 409 can, for example, be the locking mechanism of a secure door, or can be an electronic lock on a personal computer (PC) which the user 401 desires to access. A proximity card can also be used to emit the request 402, in which case the code entry module 403 has appropriate functionality.

Although the request 402 can be made secure, either by increasing the number of secret digits or by using a biometric system, the communication infrastructure in **Fig. 1** is typically less secure. The infrastructure of the arrangement 400 is generally hardwired, with the code entry module 403 generally being mounted on the outside jamb of a secured door. In such a situation, the signal path 404 can be over a significant distance in order to reach the controller 405. The path 404 represents one weak point in the security system 400, providing an unauthorised person with relatively easy access to the information being transmitted between the code entry module 403 and the controller 405. Such an unauthorised person can, given this physical access, decipher the communicated information between the code entry module 403 and the controller 405. This captured information can be deciphered, replayed in order to gain the access which rightfully belongs to the user 401, or to enable modification for other subversive purposes.

Some current systems as depicted in **Fig. 1** utilise a serial communication protocol called "Wiegand" for communication between the code entry module 403 and the controller 405. The Wiegand protocol is a simple one-way data protocol. In one known arrangement for providing secure access that uses Wiegand, the signal 404 conveyed by the code entry module 403 to the controller 405 comprises a twenty four (24) bit Wiegand protocol identifier. The Wiegand protocol can be modified by increasing or decreasing the bit count to ensure uniqueness of the protocol among different security companies. However, the Wiegand protocol does not secure the information being sent between the code entry module 403 and the controller 405. The Wiegand protocol provides no protection against interception of the signal 404 nor injection of messages into the signal 404.

More advanced protocols are known to overcome the vulnerability of the Wiegand protocol over the long distance route 404. For example, one known

arrangement for providing secure access is that distributed by Microchip Technology Inc ("the Microchip arrangement"). The Microchip arrangement is also traded under the Trade Mark, "Keeloq". The Microchip arrangement comprises multiple transmitters similar to the code entry module 403 and a receiver similar to the controller 405 described above. The code entry modules 403 of the Microchip arrangement typically reside within an insecure environment and the controller 405 resides within a secure environment. Again, authentication is based upon the transmission of a secure code in the form of a radio frequency (RF) signal over an insecure signal path similar to the signal path 404.

In the Microchip arrangement, there are typically 2^{32} different codes which may be transmitted by the code entry module 403 to the controller 405. The code entry module 403 will generate one of these secure codes from a distinct sequence, advancing progressively through the sequence on each transmission. The sequence of codes is unique for each code entry module 403 and will exhibit no apparent pattern. The transmitted code should also not include a code from any of the 2^{15} previously transmitted codes. In order to identify each code entry module 403 and a corresponding unique sequence of codes, each code entry module 403 is assigned a unique Microchip (Keeloq) serial number, which is typically twenty eight (28) bits in length. This serial number is included within each code transmission. Access will be granted by the controller 405, if a correct code is received from the code entry module 403. At any instant, the controller 405 will only accept a range of sixteen (16) codes from each code entry module's 403 sequence. Following receipt of a valid code, the sixteen code range is adjusted to coincide with the next sixteen (16) codes expected from the particular code entry module 403. This allows up to sixteen (16) transmissions to be damaged/lost before the controller 405 and the code entry module 403 become partially unsynchronised. In order to recover from a partial synchronisation loss, the controller 405 typically accepts as valid, two

consecutive codes from the 2^{15} possible codes in advance of the most recently validated code from the code entry module 403.

The Microchip arrangement achieves "unpredictability" of its codes by means of a secret "key" (typically sixty four (64) bits in length) which is known by both the code entry module 403 and the controller 405. The code entry module 403 encodes the code for transmission using an invertible encryption algorithm, customised through the application of the secret key and the Microchip (Keeloq) serial number. Accordingly, a simple ascending numerical sequence may be transformed into apparently random, uncorrelated codes, with a code sequence unique for each particular code entry module 403.

Conventionally, initial synchronisation has been established between the code entry module 403 and the controller 405 of the Microchip arrangement, by instructing the controller 405 to accept a current transmission unconditionally, without regard to the transmitted code's position within the sequence. This instruction is made through physical operation of a switch or similar mechanism located within the controller 405, while transmission is in progress. This requirement for physical operation is used to demonstrate to the controller 405 that the code entry module 103 has independent credentials for accessing the secure area, thus authorising synchronisation. Accordingly, this conventional method of synchronisation creates a weakness in the Microchip arrangement, which may be exploited by any fraudster who is be able to gain access to the secure environment of the controller 403 and synchronise a code entry module 403.

Summary

It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

According to one aspect of the present invention there is provided a system for providing secure access to a controlled item, the system comprising:

a transmitter subsystem:

means for storing a Wiegand protocol identifier;

means for receiving a request;

means for generating a code from a sequence of codes based on the Wiegand identifier, upon receiving the request;

means for encoding the code and the Wiegand protocol identifier; and

means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier; and

a receiver sub-system comprising;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier.

According to another aspect of the present invention there is provided a transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a receiver sub-system comprising means for receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal, wherein the transmitter subsystem comprises:

means for storing a Wiegand protocol identifier;

means for receiving a request;

means for generating a code from a sequence of codes based on the Wiegand protocol identifier, upon receiving the request;

WAVELYNX EX. 1003, Pg. 1415
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

means for encoding the code and the Wiegand protocol identifier; and

means for transmitting said secure access signal comprising the code and the encoded Wiegand protocol identifier embedded therein.

According to still another aspect of the present invention there is provided a receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on said Wiegand identifier, upon receiving the request, means for encoding the code and the Wiegand identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier, wherein the receiver sub-system comprises:

means for receiving the transmitted secure access signal comprising the code and the encoded Wiegand protocol identifier; and

means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier.

According to still another aspect of the present invention there is provided a method for providing secure access to a controlled item, the method comprising the steps of:

receiving a request;

generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

encoding the code and the Wiegand protocol identifier;

transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier to a controller of said controlled item; and

providing conditional access to the controlled item dependent upon said code and said Wiegand identifier.

According to still another aspect of the present invention there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to provide secure access to a controlled item, said computer program product comprising:

code for receiving a request;

code for generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

code for encoding the code and the Wiegand protocol identifier;

code for transmitting a secure access signal comprising the code and the Wiegand encoded protocol identifier to a controller of said controlled item, wherein said controller provides conditional access to the controlled item dependent upon said code and said Wiegand identifier.

According to still another aspect of the present invention there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to transmit a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a request;

code for generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

code for encoding the code and the Wiegand protocol identifier; and

code for transmitting said secure access signal comprising the code and the encoded Wiegand protocol identifier to a controller of said controlled item, wherein said

controller provides conditional access to the controlled item dependent upon said code and said Wiegand identifier.

According to still another aspect of the present invention there is provided a method of enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said method comprising the steps of:

receiving a biometric signal; and

storing a biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and

classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

According to still another aspect of the present invention there is provided an apparatus for enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal

comprising the code and the encoded Wiegand protocol identifier, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said apparatus comprising:

receiving means for receiving a biometric signal; and

storage means for storing the biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and

classification means for classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

According to still another aspect of the present invention there is provided a computer program product having a computer readable medium having a computer program recorded therein for enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said program comprising:

code for receiving a biometric signal representing a biometric signature; and

code for storing the biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and

code for classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

Other aspects of the invention are also disclosed.

Brief Description of the Drawings

Some aspects of the prior art and one or more embodiments of the present invention are described with reference to the drawings, in which:

Fig. 1 shows a prior art arrangement for providing secure access;

Fig. 2 is a functional block diagram of an arrangement for providing secure access according to the present disclosure;

Fig. 3 shows an example of a method of operation of a sub-system of **Fig. 2** comprising a code entry module, according to one embodiment;

Fig. 4 shows an example of a method of operation of the (fixed) control device of **Fig. 2**;

Fig. 5 is a schematic block diagram of the arrangement in **Fig. 2**; and

Fig. 6 shows a method of operation of the sub-system of **Fig. 2** comprising the code entry module, according to another embodiment;

Fig. 7 shows an access process relating to the example of **Fig. 6**;

Fig. 8 shows one enrolment process relating to the example of **Fig. 6**; and

Fig. 9 shows another enrolment process relating to the example of **Fig. 6**.

Detailed Description including Best Mode

It is to be noted that the discussions contained in the "Background" section relating to prior art arrangements relate to discussions of documents or devices which form public knowledge through their respective publication and/or use. Such should not be interpreted as a representation by the present inventor(s) or patent applicant that such documents or devices in any way form part of the common general knowledge in the art.

WAVELYNX EX. 1003, Pg. 1420
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Where reference is made in any one or more of the accompanying drawings to steps and/or features, which have the same reference numerals, those steps and/or features have for the purposes of this description the same function(s) or operation(s), unless the contrary intention appears.

Fig. 2 is a functional block diagram of an arrangement 100 for providing secure access according to the present disclosure. The arrangement 100 may also be referred to as a system comprising sub-systems 116 and 117. The arrangement of **Fig. 2** comprises a code entry module 103. The code entry module 103 is preferably a Microchip (Keeloq) code entry module, as described above, which is modified as described below. However, a person skilled in the art would appreciate that any other suitable type of code entry module may be used.

In the arrangement 100 of Fig. 2, a user 101 makes a request, as depicted by an arrow 102, to a controller/transmitter 107 configured within a code entry module 103. The code entry module 103 comprises a button 121 and the request 102 takes the form of a button press. A signal, as depicted by arrow 106, generated by the button press is sent to the controller/transmitter 107. Upon receiving the signal 106, the controller/transmitter 107 is configured to generate a code. In particular, the controller/transmitter 107 is configured to generate one of the 2^{32} different codes. However, the controller/transmitter 107 may be configured to generate any suitable number of different codes. The code entry module 103 will generate one of these codes from a distinct sequence, advancing progressively through the sequence on each request 102 being received. The sequence of codes is unique for each code entry module 103. Accordingly, upon receiving the signal 106, the controller/transmitter 107 checks, as depicted by an arrow 112, the current code in a database 113. The controller 107 then generates a new code in the sequence of codes for the code entry module 103.

In order to identify each code entry module 103 and the corresponding unique sequence of codes, each code entry module 103 of the present disclosure is assigned a different serial number. In the described arrangement, the Microchip (Keeloq) serial number, which is typically twenty eight (28) bits in length, is replaced by a Wiegand protocol identifier. The Wiegand protocol identifier is typically twenty four (24) bits in length. Each code entry module 103 has a different Wiegand protocol identifier. Prior to replacing the Microchip (Keeloq) serial number with the Wiegand identifier, the Wiegand protocol identifier is encoded using an invertible twenty four (24) bit encryption algorithm. Examples of encryption algorithms that may be used to encode the Wiegand protocol identifier include the Rivest, Shamir, & Adleman (RSA) algorithm, the Public Key Infrastructure (PKI) algorithm, the Data Encryption Standard (DES), Blowfish and the International Data Encryption Algorithm (IDEA). The encryption algorithm used to encode the Wiegand protocol identifier is known only to the code entry module 103 and to a receiver 118, as seen in Fig. 2, which will be described below.

The encoded Wiegand protocol identifier is inserted into bits zero (0) to twenty three (23) of the normal Microchip (Keeloq) serial number address space for the code entry module 103. The remaining four bits (i.e., bits twenty four (24) to twenty seven (27)) of the Microchip (Keeloq) serial number are set to a predetermined fixed value (e.g., a series of '1's) indicating that the Microchip (Keeloq) serial number has been replaced by an encoded Wiegand protocol identifier. The Wiegand protocol identifier is allocated entirely within a predetermined ($1/16^{th}$) portion of the normal Microchip (Keeloq) code entry module (or transmitter) address space for the code entry module 103. A person skilled in the art would appreciate that the Wiegand protocol identifier may be inserted into any suitable bits of the normal Microchip (Keeloq) serial number address space for

the code entry module 103. Further, any bits may be used to indicate that the Microchip (Keeloq) serial number has been replaced by the Wiegand protocol identifier.

Each code entry module 103 has a Wiegand protocol identifier allocated to the code entry module 103 prior to the code entry module 103 being distributed to the user 101 for use. The Wiegand protocol identifier may be stored in the database 113. Prior to the code entry module 103 being distributed to the user 101, the code entry module 103 is also allocated a secret "key" (typically sixty four (64) bits in length) which is known by both the code entry module 403 and the receiver 118. Again, the secret key may be stored in the database 113 on the transmitter sub-system 116. The secret key may also be stored in a database 115 on the receiver sub-system 117.

Upon generating the new code in the sequence of codes for the code entry module 103, the controller 107 sends the updated code, this being referred to as an access signal, as depicted by an arrow 108 to the receiver 118. Prior to the new code being sent to the controller 109, the new code is preferably encoded by the controller 107 using one of the encryption algorithms described above with the encryption algorithm being customised through the application of the secret key and the Wiegand protocol identifier. The encoded Wiegand protocol identifier number for the code entry module 103 is also included within the access signal 108.

The receiver 118 receives the access signal 108 and firstly determines that the four bit fixed portion of the address space for a Microchip (Keeloq) serial number correctly indicates that the serial number has been replaced by an encoded Wiegand protocol identifier. If the receiver 118 determines that the four bit fixed portion does not indicate that the Microchip (Keeloq) serial number has been replaced by an encoded Wiegand protocol identifier then the receiver 118 rejects the access signal 108. Otherwise, the receiver 118 decodes the code included in the access signal 108, using the

encryption algorithm that was used by the code entry module 103 to encode the code. The receiver also decodes the Wiegand protocol identifier using the encryption algorithm that was used by the code entry module 103 to encode the Wiegand protocol identifier.

Based on the decoded Wiegand protocol identifier, the receiver 118 identifies the sequence of codes being used by the code entry module 103 and tests the code received in the access signal 108 against the most recent previously received code for the code entry module 103, this code having been stored in the database 115, this testing being depicted by an arrow 114. As will be described in detail below, the codes are stored in the database 115 in a hash table, or similar data structure. The receiver 118 uses the Wiegand protocol identifier received with the access signal 108 and linear probing for accessing the codes stored in the hash table in order to test the code received in the access signal 108.

If the code within the received access signal 108 is found to be the next code in the sequence for the received Wiegand protocol identifier, then, the receiver 118 provides a signal 120, in Wiegand format, to the controller 109. The signal 120 includes the decoded Wiegand identifier. In response to the signal 120, the controller 109 sends a command, as depicted by an arrow 110, to a controlled item 111. The controlled item 111 may be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user 101.

It is noted that the receiver 118 receives the transmitted access signal 108 and converts it into a form that the controller 109 can use, as depicted by the arrow 120. As the Wiegand protocol identifier is allocated entirely within a predetermined portion of the normal address space for Microchip (Keeloq) code entry modules (or transmitters) of the code entry module 103, the receiver 118 may be a conventional Microchip (Keeloq) receiver. However, such a conventional Microchip (Keeloq) receiver is modified so as to

use the Wiegand protocol identifier received with the access signal 108 for accessing the codes stored in the hash table.

The sub-system 117 maintains a unique sequence of codes for each of the code entry modules that the receiver 118 may encounter. Each of these code entry modules has a unique Wiegand protocol identifier corresponding to one of the sequences. The total number of possible code entry modules, each having a unique Wiegand identifier, and accordingly, the total number of unique code sequences, is 2^{24} (i.e., more than 16 million). A person skilled in the relevant art would appreciate that more or less code sequences may be possible. Each of these code sequences is stored in the database 115. In order to provide sufficient access for the receiver 118 to the stored codes, the codes are stored in a hash table or similar data structure within the database 115, as described above. The receiver 118 may use a "hash table with linear probing" algorithm, as described above, to access the codes within the data structure. This allows the codes to be stored within a physical storage area of a size proportional to the number of active code entry modules. Such a hash table algorithm also requires the selection of a "hash function." The 24 bit Wiegand protocol identifier may be used as this hash function.

The code entry module 103 may also incorporate at least one mechanism for providing feedback to the user 101. This mechanism may, for example, take the form of one or more Light Emitting Diodes (LEDs) 122 which can provide visual feedback, depicted by an arrow 123 to the user 101. Alternately or in addition the mechanism can take the form of an audio signal provided by an audio transducer 124 providing audio feedback 125.

The codes generated by the code entry module 103 may be referred to as "rolling codes". Rolling codes provide a substantially non-replayable, non-repeatable and encrypted radio frequency data communications scheme for secure messaging. These

codes use inherently secure protocols and serial number ciphering techniques which in the present disclosure hide the clear text values required for authentication between the key fob (transmitter) sub-system 116 and the receiver/controller 118/109.

As described above, the rolling codes generated by the code entry module 103 use a different code variant each time the transmission of the access signal 108 occurs. This is achieved by encrypting the data from the controller 107 with an encryption algorithm, as described above, and ensuring that successive transmissions of the access signal 108 are modified using a code and/or a look-up table or hash table known to both the transmitter sub-system 116 and the receiver sub-system 117. Using this approach, successive transmissions are modified, resulting in a non-repeatable data transfer, even if the information from the controller 107 remains the same. The modification of the code in the access signal 108 for each transmission significantly reduces the likelihood that an intruder can access the information and replay the information to thereby gain entry at some later time.

As described above, based on the Wiegand protocol identifier, the receiver 118 identifies the sequence of codes being used by the code entry module 103 and tests the code received in the access signal 108 against the most recent previously received code for the code entry module 103, this code having been stored in the database 115, this testing being depicted by the arrow 114. If the incoming code forming the access signal 108 is found "not to be" the next code in the sequence for that code entry module 103, then the receiver 118 stores the Wiegand protocol identifier received in the access signal 108. The receiver 118 also then stores another code which is the next code expected in the sequence (the "expected next code") for the code entry module 103 (i.e., as identified by the Wiegand protocol identifier) after the code that was received in the access signal 108. The receiver 118 also starts a timer for a predetermined time. If another access signal 108

is received from the same code entry module 103 within the predetermined time and the code in the access signal 108 exactly matches the "expected next code" as previously stored, then the receiver 118 provides the signal 120 in the Wiegand format to the controller 109. The receiver 118 also stores a flag in the database 115 indicating that the receiver 118 and the code entry module 103 are "synchronised". Accordingly, the code entry module 103 and the receiver 118 may be synchronised provided the code entry module 103 can generate two consecutive "in sequence" codes.

The above method of synchronising the code entry module 103 and the receiver 118 is particularly advantageous over conventional Microchip (Keeloq) secure access arrangements using conventional Microchip (Keeloq) code entry modules (or transmitters), which require physical operation of a switch mechanism in a receiver. The arrangement 100 described above can maintain security without the need to demonstrate physical access during synchronisation, since the arrangement 100 guarantees the authenticity of the code entry module 103, and hence the authenticity of the resultant Wiegand protocol identifiers.

The sub-system in **Fig. 2** falling to the left hand side, as depicted by an arrow 116, of a dashed line 119 may be implemented in a number of different forms. The sub-system 116 may for example be incorporated into a remote fob (which is a small portable device carried by the user 101), or alternately may be mounted in a protected enclosure on the outside jamb of a secured door. The sub-system 116 communicates with the sub-system 117 on the right hand side of the dashed line 119 via the wireless communication channel used by the access signal 108. The sub-system 117 is typically located in an inaccessible area such as a hidden roof space or alternately in a suitable protected area such as an armoured cupboard. The location of the sub-system 117 must of course be consistent with reliable reception of the wireless access signal 108.

Although typically the communication channel uses a wireless transmission medium, there are instances where the channel used by the access signal 108 may use a wired medium. This is particularly the case when the transmitter sub-system 116 is mounted in an enclosure on the door jamb rather than in a portable key fob.

In the event that the sub-system 116 is implemented as a remote fob, the combination of the Wiegand identifier and the strongly encrypted wireless communication provides a particularly significant advantage over conventional secure access arrangements. The remote key fob arrangement allows easy installation, since the wired communication path 404 (see **Fig. 1**) is avoided. Other existing wiring elements of the present systems 400 may be used where appropriate.

Fig. 3 shows the method of operation of the sub-system 116 of **Fig. 2** comprising the code entry module 103. The process 200 commences with a testing step 201 in which the code entry module 103 checks whether a request 102 is being received. If this is not the case, then the method 200 is directed in accordance with a NO arrow back to the step 201 in a loop. If, on the other hand, the request 102 has been received, then the method 200 is directed in accordance with a YES arrow to a step 202. In the step 202, the controller/transmitter 107 checks, as depicted by an arrow 112, the current code in the database 113. Then at the next step 203, the controller/transmitter 107 generates a new code in the sequence of codes for the code entry module 103 according to the Wiegand protocol identifier allocated to the code entry module 103.

At the next step 204, the newly generated code is encoded by the controller/transmitter 107 using one of the encryption algorithms described above, with the encryption algorithm being customised through the application of the secret key and the Wiegand protocol identifier. The Wiegand identifier is also encrypted at step 204, using one of the encryption algorithms described above. In the subsequent step 205, the

controller 107 sends the appropriate access signal 108 to the receiver 109. The access signal comprises the encoded code and the encoded Wiegand protocol identifier. The process 200 is then directed in accordance with an arrow 206 back to the step 201.

Fig. 4 shows the method of operation of the control sub-system 117 of **Fig. 2**. The process 300 commences with a testing step 301 which continuously checks whether the access signal 108 has been received from the controller/transmitter 107. The step 301 is performed by the receiver 118. As long as the access signal 108 is not received the process 300 is directed in accordance with a NO arrow in a looping manner back to the step 301. When the access signal 108 is received, the process 300 is directed from the step 301 by means of a YES arrow to a step 302. In the step 302, if the receiver 118 determines that the four bit fixed portion following the Wiegand protocol identifier included in the received access signal 108 correctly indicates that the serial number has been replaced by an encoded Wiegand protocol identifier, then the process 300 is directed from the step 302 by means of a YES arrow to a step 303. Otherwise, the process 300 is directed in accordance with a NO arrow in a looping manner back to the step 301.

At step 303, the receiver 118 decodes the code included in the access signal 108, using the encryption algorithm that was used to encode the code. The receiver 118 also decodes the Wiegand protocol identifier included in the signal 108. Then at step 304, the receiver 118 identifies the sequence of codes being used by the code entry module 103, based on the Wiegand protocol identifier, and tests the code received in the access signal 108 against the most recent previously received code for the code entry module 103, this code having been stored in the database 115. If the incoming code forming the access signal 108 is found to be the next code in the sequence corresponding to the Wiegand protocol identifier included in the access signal 108, then the process 300 is directed from the step 304 by means of a YES arrow to a step 305. In step 305, the receiver 118

provides the signal 120 in the Wiegand format to the controller 109. The signal 120 comprises the Wiegand protocol identifier.

In a subsequent step 308, the controller 109 sends a control signal 110 to the controlled item 111 (for example opening a secured door). The process 300 is then directed from the step 308 as depicted by an arrow 308 back to the step 301.

Returning to the testing step 304, if the incoming code forming the access signal 108 is found "not to be" the next code in the sequence corresponding to the Wiegand protocol identifier included in the received access signal 108, then the process 300 is directed from the step 304 by means of the NO arrow to step 306. At step 306, the receiver 118 determines what the next code in the sequence corresponding to the Wiegand protocol identifier after the code that was received in the access signal 108 at step 301. This next code is the "next expected code" as described above. Then at the next step 309, the receiver 118 stores the code entry module's 103 Wiegand protocol identifier and the code determined at step 306 (i.e., the next expected code) in the database 115. The receiver 118 also starts a timer to time out for a predetermined time (e.g., ten (10) seconds).

In a subsequent step 310, if another access signal 108 is received from the same code entry module 103 (i.e., the access signal 108 contains the encoded Wiegand protocol identifier corresponding to the code entry module 103) within the predetermined time, then the process 300 is directed from the step 310 by means of the YES arrow to step 311. Otherwise, the process 300 is directed from the step 310 by means of the NO arrow back to step 301. At step 311, if the incoming code included in the access signal 108 received at step 310 is found to be the code stored at step 309 (i.e., the next expected code), then the process 300 is directed from the step 311 by means of a YES arrow to step 307. Otherwise, the process 300 is directed from the step 311 by means of the NO arrow back

to step 301. Accordingly, the code entry module 103 and the receiver 118 may be synchronised provided the code entry module 103 can generate two consecutive "in sequence" codes.

One of the advantages of the arrangement 100 described above is that security system upgrades may be made without replacing the Wiegand compatible controller 109. Accordingly, existing systems as are described in **Fig. 1** may be upgraded by replacing the code entry module 403 and the transmission path 404, leaving the other components of the system 400 (ie., the controller 405, the code database 407, and the controlled item 409, together with existing wiring 408 and 406), largely intact. Minor programming modifications may however be necessary to the receiver 118 so that the receiver 118 uses the Wiegand protocol identifier to interrogate the hash table stored in the database 115. When upgrading systems in this manner, the sub-system 116 may either be used in a remote fob configuration, or may be placed in a secure housing on an external door jamb.

In the code entry module 103 described above, the code entry module 103 comprises a button 121 and the request 102 takes the form of a button press. In another embodiment as described below, the code entry module 103 may comprise a biometric sensor (not shown), either in place of the button 121 or as well as the buttons 121, and the request 102 may take a form which corresponds to the nature of the biometric sensor in the module 103.

In accordance with the further embodiment described below of the arrangement 100, the button 121 is replaced by a biometric sensor which will be referred to below as the "biometric sensor 121". If the biometric sensor 121 in the code entry module 103 is a fingerprint sensor, then the request 102 typically takes the form of a thumb press on a sensor panel (not shown) on the code entry module 103. In this instance, the code entry module 103 would interrogate, as depicted by an arrow 104, a user identity database 105.

Thus, for example, if the request 102 is the thumb press on the biometric sensor 121 then the user database 105 contains biometric signatures for authorised users against which the request 102 can be authenticated. If the identity of the user 101 is authenticated successfully, then the code entry module 103 sends the signal 106 to the controller/transmitter 107. Then, as at step 202, in response to receiving the signal 106, the controller/transmitter 107 checks, as depicted by the arrow 112, the current code in the database 113. The controller/transmitter 107 then generates a new code in the sequence of codes for the code entry module 103, as at step 203. As described above, the newly generated code is encrypted by the controller/transmitter 107 using one of the encryption algorithms described above. The controller 107 then sends the appropriate access signal 108 to the receiver 109, as at step 205.

The biometric signature database 105 is shown in **Fig. 2** to be part of the transmitter sub-system 116. However, in an alternate arrangement, the biometric signature database 105 may be located in the receiver sub-system 117, in which case the communication 104 between the code entry module 103 and the signature database 105 may also be performed over a secure wireless communication channel such as the one used by the access signal 108. In the event that the secure access arrangement 100 is being applied to providing secure access to a PC, then the secured PC may store the biometric signature of the authorised user in internal memory, and the PC may be integrated into the receiver sub-system 117 of **Fig. 2**.

In addition to authenticating the user 101, the biometric sensor 121 in the code entry module 103 in conjunction with the controller 107 may also check other access privileges of the user 101. These access privileges may be contained in the database 105 which may be located either locally in the remote key fob, or in the receiver sub-system 117 as previously described. In one example, Tom Smith may firstly be authenticated as

Tom Smith using the thumb press by Tom on the biometric sensor panel (not shown). After Tom's personal biometric identity is authenticated, the transmitter sub-system 116 may check if Tom Smith is in fact allowed to use the particular door secured by the device 111 on weekends. Thus the security screening offered by the described arrangement may range from simple authentication of the user's identity, to more comprehensive access privilege screening.

The incorporation of the biometric sensor 121 into the code entry module 103 in the form of a remote key fob also means that if the user 101 loses the remote key fob, the user need not be concerned that someone else can use the code entry module 103. Since the finder of the lost key fob will not be able to have his or her biometric signal authenticated by the biometric sensor 121 in the code entry module 103, the lost key fob is useless to anyone apart from the rightful user 101.

The transmitter sub-system 116 is preferably fabricated in the form of a single integrated circuit (IC) to reduce the possibility of an authorised person bypassing the biometric sensor 121 in the code entry module 103 and directly forcing the controller 107 to emit the access signal 108.

The incorporation of the biometric sensor 121 into the code entry module 103, as described above, allows the user 101 to be validated. In this manner, the transmissions of the access signal 108 containing the encrypted code and Wiegand protocol identifier may be limited to occur for only authorised users. The incorporation of the biometric sensor 121 into the code entry module 103, also allows the security of the arrangement of **Fig. 2** to be maintained without the reliance on the physical security of the code entry modules. However, the incorporation of the biometric sensor 121 also creates the need for a method of allowing the enrolment of the user's biometrics.

Fig. 6 shows another process 700 of operation of the arrangement 100 of Fig. 2 where the code entry module 103 incorporates the biometric sensor 121, in accordance with the further embodiment. In this further embodiment, the process 700 is performed instead of the process 200 of Fig. 3. The code entry module 103 incorporating the biometric sensor 121 is allocated a range of Wiegand protocol identifiers rather than just one Wiegand protocol identifier as with the first embodiment described above. The Wiegand protocol identifier in this range are distinct from those allocated to other code entry modules sharing the same "secret" key as described above. The Wiegand protocol identifier being used at any particular time is referred to as the "current" Wiegand protocol identifier.

The process 700 commences with a step 701 that determines if a biometric signal has been received by the biometric sensor 121 in the code entry module 103. If not, then the process 700 follows a NO arrow back to the step 701. If however a biometric signal has been received, then the process 700 follows a YES arrow to a step 702 that determines if the user ID database 105 in **Fig. 2** is empty. This would be the case, for example, if the code entry module is new and has never been used, or if the user 101 has erased all the information in the database 105 (as will be described in detail below).

If the database 105 is empty, then the process 700 is directed by an arrow 703 to 706 in **Fig. 8** which depicts a process 800 dealing with the enrolment or the administration function for loading relevant signatures into the database 105. If on the other hand the database 105 is not empty, then the process 700 is directed to a step 704 that determines if the biometric signal that has been received is an administrator's biometric signal.

The arrangement 100 comprising the code entry module 103 incorporating the biometric sensor 121 may accommodate at least three classes of user, namely

administrators, (ordinary) users, and duress users. The administrators have the ability to amend data stored, for example, in the database 105, while the ordinary users preferably do not have this capability. The first user of the code entry module 103, whether this is the user who purchases the module, or the user who programs the module 103 after all data has been erased from the database 105, is automatically categorised as an administrator. This first administrator may direct the arrangement 100 to either accept further administrators, or alternately to only accept further ordinary users.

Although the present description refers to "users", in fact it is "fingers" which are the operative entities in operation of the arrangement 100 where the biometric sensor 121 is a fingerprint sensor. In this event, a single user may enrol two or more of his or her own fingers as separate administrators or (ordinary) users of the arrangement 100, by storing corresponding fingerprints for corresponding fingers in the database 105 via the enrolment process 800 (see **Fig. 8**).

Some class overlap is possible. Thus a stored biometric signature can belong to an administrator in the duress class.

The first administrator may provide control information to the code entry module 103 by providing a succession of finger presses to the biometric sensor 121, providing that these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time. In one arrangement, the control information is encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses. If the successive finger presses are provided within this predetermined time, then the controller 107 accepts the presses as potential control information and checks the input information against a stored set of legal control signals.

One example of a legal control signal can be expressed as follows:

"Enrol an ordinary user" -> dit, dit, dit, dah

where "dit" is a finger press of one second's duration (provided by the user 101 in response to the feedback provided by the Amber LED as described below), and "dah" is a finger press of two second's duration.

In the event that a legitimate sequence of finger presses are not delivered within the predetermined time, then the presses are considered not to be control information and merely to be presses intended to provide access to the controlled item 111. Legitimate control sequences are defined in Read Only Memory (ROM) in the controller 107.

The code entry module 103 has feedback signalling mechanisms 122, implemented for example by a number of LEDs 122 and an audio transducer 124, implemented by an audio transducer. The LEDs 122 and the audio transducer 124 are used by the controller to signal the state of the code entry module 103 to the user 101, and to direct the administration process. Thus, in one example, three LEDs, being Red, Amber and Green are provided.

When the Amber LED is flashing, it means "Press the sensor". When the Amber LED is steady ON, it means "Maintain finger pressure". When the Amber LED is OFF, it means "Remove finger pressure". When the arrangement 100 enters the enrolment state (depicted by the process 800 in **Fig. 8**), then the audio transducer 124 emits the "begin enrolment" signal (*dit dit dit dit*) and the Red LED flashes. Enrolment of a normal user (according to the step 807 in **Fig. 8**) is signalled by the OK audio signal (*dit dit*) and a single blink of the Green LED.

Returning to the step 704, if the step determines that the biometric signal received is an administrator's signal, then the process 700 is directed by a YES arrow to 706 in **Fig. 8** as depicted by the arrow 703. If on the other hand, the step 704 indicates that the received biometric signal does not belong to an administrator then the process 700 is directed by a NO arrow to 707 in **Fig. 7**.

Fig. 7 shows the access process 600 by which a biometric signal 102 (see **Fig. 2**) is processed in order to provide access to the controlled item 111, or to take other action. Entering the process at 707 from **Fig. 6**, the process 600 proceeds to a step 602 that compares the received biometric signal to biometric signatures stored in the database 105. A following step 603 determines if the received signal falls into the "duress" category. Biometric signals in this category indicate that the user 101 is in a coercive situation where, for example, an armed criminal is forcing the user 101 to access the secure facility (such as a bank door). If the step 603 determines that the received biometric signal is in the duress class, then a following step 604 prepares a "duress" bit for incorporation into the code access signal 108. The aforementioned duress bit is an access attribute of the biometric signal 102. Thereafter the process 600 proceeds to a step 605.

Modules used in the code entry module for producing the rolling code enable a number of user defined bits to be inserted into the access signal 108, and these bits may be used to effect desired control functions in the receiver sub-system 117. The disclosed arrangement 100 utilises four such user bits, namely (a) to indicate that the user belongs to the duress category, (b) to indicate a "battery low" condition, or other desired system state or "telemetry" variable, for the code entry module 103, (c) to indicate that the biometric signal represents a legitimate user in which case the secure access to the controlled item 111 is to be granted, or (d) to indicate that the biometric signal is unknown, in which case the controller 109 in the receiver sub-system 117 sounds an alert tone using a bell (not shown) or the like.

Returning to **Fig. 7**, if the step 603 determines that the biometric signal is not in the duress class, then the process 600 proceeds according to a NO arrow to the step 605. The step 605 determines if the code entry module 103 has a low battery condition, in which event the process 600 proceeds according to a YES arrow to a step 606 that

prepares a telemetry bit for insertion into the access signal 108. The aforementioned telemetry bit is an access attribute of the biometric signal 102. Thereafter, the process proceeds to a step 607.

If the step 605 determines that telemetry signalling is not required, then the process 600 proceeds according to a NO arrow to the step 607. The step 607 checks the biometric signal against the biometric signatures in the database 105. If the received biometric signal matches a legitimate signature in the database 105, then the process 600 is directed to a step 608 that prepares an "access" bit for insertion into the access signal 108. This access bit directs the controller 109 in the receiver sub-system 117 to provide access to the controlled item 111. The aforementioned access bit is an access attribute of the biometric signal 102. The process 600 then proceeds to a step 610.

If the step 607 determines that the biometric input signal does not match any legitimate biometric signatures in the database 105, then the process 600 proceeds according to a NO arrow to a step 609 that prepares an "alert" bit for insertion into the access signal 108. The aforementioned alert bit is an access attribute of the biometric signal 102. This alert bit directs the controller 109 (a) not to provide access to the controlled item 111, and (b) to provide an alert tone, like ringing a chime or a bell (not shown), to alert personnel in the vicinity of the receiver sub-system 117 that an unauthorised user is attempting to gain access to the controlled item 111. The alert bit may also cause a camera mounted near the controlled item 111 to photograph the unauthorised user for later identification of that person. The camera may be activated if the person attempting to gain access is unauthorised, and also if the person attempting to gain access is authorised but uses a duress signature.

An optional additional step (not shown) may prepare an identification field for insertion into the access signal 108. This sends, to the receiver sub-system 117, ID

information that the receiver sub-system 117 may use to construct an audit trail listing which users, having signatures in the database 105, have been provided with access to the controlled item 111.

The process 600 is then directed to the step 610, where the controller/transmitter 107 checks, as depicted by an arrow 112 in **Fig. 2**, the current code in the database 113. Then at the next step 613, the controller/transmitter 107 generates a new code in the sequence of codes for the code entry module 103 according to the current Wiegand protocol identifier. At the next step 615, the newly generated code is encoded by the controller 107 using one of the encryption algorithms described above, with the encryption algorithm being customised through the application of the secret key and the current Wiegand protocol identifier. The Wiegand identifier is also encoded at step 204, using one of the encryption algorithms described above. In the subsequent step 617 the controller/transmitter 107 sends the appropriate access signal 108 to the receiver 109. The access signal 108 includes the encoded code and the current encoded Wiegand protocol identifier. Also, in the embodiment of Figs. 7 to 9, the access signal 108 also includes the various user defined bits. The process 200 is then directed in accordance with an arrow 611 to 705 of Fig. 6.

. **Fig. 8** shows a process 800 for implementing various enrolment procedures. The process 800 commences at 706 from **Fig. 6** after which a step 801 determines if the biometric signal is a first administrator's signal (which is the case if the database 105 is empty). If this is the case, then the process 800 is directed to a step 802 that stores a biometric signature, representing the received biometric signal, in the database 105. From a terminology perspective, this first administrator, or rather the first administrator's first finger (in the event that the biometric sensor 121 is a fingerprint sensor), is referred to as the "superfinger". Further administrator's fingers are referred to as admin-fingers, and

ordinary users fingers are referred to merely as "fingers". The reason that someone would enrol more than one of their own fingers into the system is to ensure that even in the event that one of their enrolled fingers is injured, the person can still operate the system using another enrolled finger.

It is noted that the step 802, as well as the steps 805, 807 and 809 involve sequences of finger presses on the biometric sensor 121 in conjunction with feedback signals from the LEDs 122 and/or the audio speaker 124. The process 800 then proceeds to a step 810 that determines if further enrolment procedures are required. If this is the case, then the process 800 proceeds by a YES arrow back to the step 801. If no further enrolment procedures are required, then the process 800 proceeds by a NO arrow to 705 in **Fig. 6**.

Returning to the step 801, if the biometric signal is not a first administrator's signal, then the process 800 proceeds by a NO arrow to a step 803. The step 803 determines if a further administrator signature is to be stored. It is noted that all signatures stored in the database are tagged as belonging to one or more of the classes of administrator, ordinary user, and duress users. If a further administrator signature is to be stored, then the process 800 proceeds by a YES arrow to the step 802 that stores the biometric signal as a further administrator's signature.

If a further administrator's signature is not required, then the process 800 proceeds according to a NO arrow to a step 804 that determines if a duress signature is to be stored. If this is the case then the process 800 follows a YES arrow to a step 805 that stores a duress signature. The process 800 then proceeds to the step 810. If however the step 804 determines that a duress signature is not required, then the process 800 proceeds by a NO arrow to step 806.

The step 806 determines if a further simple signature (i.e., belonging to an ordinary user) is to be stored. If a further simple signature is to be stored, then the process 800 proceeds by a YES arrow to the step 807 that stores a representation of the received biometric signal as a further ordinary signature.

If a further simple signature is not required, then the process 800 proceeds according to a NO arrow to a step 808 that determines if any or all signatures are to be erased from the database 105. The determination of whether all signatures are to be erased from the database 105 at step 808 may be made based on an "erase all" control (not shown) incorporated into the code entry module 103. If any or all signatures are to be erased from the database 105 then the process 800 follows a YES arrow to a step 809 that erases the desired signatures.

If all of the signatures in the database 115 are erased at step 809, the controller/transmitter 107 changes the current Wiegand protocol identifier to a previously unused value from the range of Wiegand protocol identifiers allocated to the code entry module 103. If no previously unused values from the range of Wiegand protocol identifiers allocated to the code entry module 103 are available, then the code entry module 103 is completely non-functional and the process 800 concludes at step 809 and will not return to 705 of Fig. 6.

If all of the signatures in the database 115 are erased at step 809, the database 115 will be determined to be empty at a subsequent execution of step 702 of the process 700. Further, the code entry module 103 will appear as completely new to the receiver 118 and any existing synchronisation between the code entry module 103 and the receiver 118 will be revoked. That is, the flag in the database 115 indicating that the receiver 118 and the code entry module 103 are "synchronised" will be reset to indicate that the code entry module 103 and the receiver 118 are not synchronised. In the instance that

synchronisation is revoked as described above, the code entry module 103 and the receiver 118 may be synchronised provided the code entry module 103 can generate two consecutive "in sequence" codes or through physical operation of a switch mechanism as described above.

If the code entry module 103 is still functional (i.e., there are still unused values from the range of Wiegand protocol identifiers allocated to the code entry module 103) following step 809, then the process 800 then proceeds to the step 810.

Further, if the step 804 determines that no signatures are to be erased, then the process 800 proceeds by a NO arrow to the step 810.

Fig. 9 shows another enrolment process relating to the example of **Fig. 6**. The process 900 commences at 706 from **Fig. 6** after which a step 901 determines if the received biometric signal comes from the first administrator. If this is the case, then the process 900 proceeds according to a YES arrow to a step 902. The step 902 emits an "Enrolment" tone and flashes the green LED once only. Thereafter, a step 905 reads the incoming biometric signal which is provided by the user as directed by the Amber LED. When the Amber LED flashes continuously, this directs the user to "Apply Finger". When the Amber LED is in a steady illuminated state, this directs the user to "Maintain Finger Pressure". Finally, when the amber LED is off, this directs the user to "Remove Finger".

Returning to the step 901, if the incoming biometric signal does not belong to the first administrator, then the process 900 proceeds according to a NO arrow to a step 903. The step 903 emits an "Enrolment" tone, and flashes the Red LED in an on-going fashion. Thereafter, the process 900 proceeds according to an arrow 904 to the step 905.

Following the step 905, a step 906 determines whether the incoming biometric signal is legible. If this is not the case, then the process 900 proceeds according to a NO

arrow to a step 907. The step 907 emits a "Rejection" tone, after which the process 900 is directed, according to an arrow 908 to 705 in **Fig. 6**. Returning to the step 906, if the incoming biometric signal is legible, then the process 900 follows a YES arrow to a step 909. The step 909 determines whether the finger press exceeds a predetermined time. If this is not the case, then the process 900 follows a NO arrow to a step 910 which stores a representation of the biometric signal, which in the present case is stored as a fingerprint signature. Thereafter the process 900 follows an arrow 911 to 705 in **Fig. 6**.

Returning to the step 909 if the finger press does exceed the predetermined period, then the process follows a YES arrow to a step 912. The step 912 erases any or all relevant signatures depending upon the attributes of the incoming biometric signal. Thus, for example, if the incoming biometric signal belongs to an ordinary user, then the ordinary user's signature in the database 105 is erased by the step 912. If, on the other hand, the incoming biometric signal belongs to the first administrator, then all the signatures in the database 105 are erased. Administrators who are not the first administrator may be granted either the same powers as the first administrator in regard to erasure of signatures, or can be granted the same powers as ordinary user in this respect.

Again, the determination of whether all signatures are to be erased from the database 105 at step 912 may be made based on an "erase all" control (not shown) incorporated into the code entry module 103. Further, if all of the signatures in the database 115 are erased at step 912, the controller/transmitter 107 changes the current Wiegand protocol identifier to a previously unused value from the range of Wiegand protocol identifiers allocated to the code entry module 103. If no previously unused values from the range of Wiegand protocol identifiers allocated to the code entry module 103 are available, then the code entry module 103 is completely non-functional and the process 900 concludes at step 912 and will not return to 705 of Fig. 6.

If the code entry module 103 is still functional (i.e., there are still unused values from the range of Microchip (Keeloq) serial numbers allocated to the code entry module 103) following step 912, then the process 900 follows an arrow 913 to 705 in **Fig. 6**.

Fig. 5 is a schematic block diagram of the arrangement 100 in **Fig. 2**. The disclosed secure access methods are preferably practiced using the arrangement 100 in the form of a computer system, such as that shown in **Fig. 5** wherein the processes of **Figs. 3-4** and **6-9** may be implemented as software, such as application program modules executing within the arrangement 100. In particular, the described method steps are effected by instructions in the software that are carried out under direction of the respective controller 107 and controller 109 (and receiver 118) in the transmitter and receiver sub-systems 116 and 117. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part performs the provision of secure access methods and a second part manages a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described below, for example. The software is loaded into the transmitter and receiver sub-systems 116 and 117 from the computer readable medium, and then executed under direction of the respective controllers 107 and 109 (and receiver 118). A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the computer preferably effects an advantageous apparatus for provision of secure access.

The following description is directed primarily to the transmitter sub-system 116, however the description applies in general to the operation of the receiver sub-system 117. The arrangement 100 is formed, having regard to the transmitter sub-system 116, by the controller module 107, input devices such as the button 121 (or biometric sensor in

the case of the further embodiment), output devices including the LED display 122 and the audio device 124. A communication interface/transceiver 1008 is used by the controller module 107 for communicating to and from a communications network 1020. Although **Fig. 2** shows the transmitter sub-system 116 communicating with the receiver sub-system 117 using a direct wireless link for the access signal 108, this link used by the access signal 108 can be effected over the network 1020 forming a tandem link comprising 108-1020-108'. The aforementioned communications capability may be used to effect communications between the transmitter sub-system 116 and the receiver sub-system 117 either directly or via the Internet, and other network systems, such as a Local Area Network (LAN) or a Wide Area Network (WAN).

The controller module 107 typically includes at least one processor unit 1005, and a memory unit 1006, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The controller module 107 also includes a number of input/output (I/O) interfaces including an audio-video interface 1007 that couples to the LED display 122 and audio speaker 124, an I/O interface 1013 for the button 121, and the interface 1008 for communications. The components 1007, 1008, 1005, 1013 and 1006 of the controller module 107 typically communicate via an interconnected bus 1004 and in a manner which results in a conventional mode of operation of the controller 107 known to those in the relevant art.

Typically, the application program modules for the transmitter sub-system 116 are resident in the memory 1006 iROM, and are read and controlled in their execution by the processor 1005. Intermediate storage of the program and any data fetched from the bio sensor 121 and the network 1020 may be accomplished using the RAM in the semiconductor memory 1006. In some instances, the application program modules may be supplied to the user encoded into the ROM in the memory 1006. Still further, the

software modules can also be loaded into the transmitter sub-system 116 from other computer readable media, say over the network 1020. The term "computer readable medium" as used herein refers to any storage or transmission medium that participates in providing instructions and/or data to the transmitter sub-system 116 for execution and/or processing. Examples of storage media include floppy disks, magnetic tape, CD-ROM, a hard disk drive, a ROM or integrated circuit, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the transmitter sub-system 116. Examples of transmission media include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

As described above, the code entry module 103 incorporating the biometric sensor 121 is allocated a range of Wiegand protocol identifiers. In still another arrangement, the code entry module 103 may comprise a plurality of buttons similar to the button 121 shown in Fig. 2. In this instance, each of these buttons may have a different Wiegand protocol identifier, with each Wiegand identifier having a unique sequence of codes. Accordingly, pressing different ones of the buttons will result in different codes being sent by the code entry module 103.

As described above, the encoded Wiegand protocol identifier is inserted into bits zero (0) to twenty three (23) of the normal Microchip (Keeloq) serial number address space for the code entry module 103. The remaining four bits (i.e., bits twenty four (24) to twenty seven (27)) of the Microchip (Keeloq) serial number are set to a predetermined fixed value (e.g., a series of '1's) indicating that the Microchip (Keeloq) serial number has been replaced by an encoded Wiegand protocol identifier. Alternatively, two or more of the remaining four bits may be may be used to indicate user groups. In this instance,

the code entry module 103 will only be accepted by the receiver 118 if the code entry module 103 and the receiver 118 are in the same user group. In one example, bits twenty six (26) and twenty seven (27) may be set to '1', while the remaining two bits (i.e., bits twenty four (24) and twenty five (25)) are set to a user group number.

Code entry modules may also be allocated to different user groups by using a different secret key, as described above, in each of the code entry modules. For example, one or more of the code entry modules may be allocated a particular secret key indicating one user group and one or more other code entry modules may be allocated a different secret key indicating a different user group.

Industrial Applicability

It is apparent from the above that the arrangements described are applicable to the security industry.

The foregoing describes only some embodiments of the present invention, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

The arrangement 100 may also be used to provide authorised access to lighting systems, building control devices, exterior or remote devices such as air compressors and so on. The concept of "secure access" is thus extendible beyond mere access to restricted physical areas.

Claims

1. A system for providing secure access to a controlled item, the system comprising:

a transmitter subsystem:

means for storing a Wiegand protocol identifier;

means for receiving a request;

means for generating a code from a sequence of codes based on the Wiegand identifier, upon receiving the request;

means for encoding the code and the Wiegand protocol identifier; and

means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier; and

a receiver sub-system comprising;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier.

2. A system according to claim 1, wherein the sequence of codes is unique to the transmitter sub-system.

3. A system according to claim 1, wherein the Wiegand protocol identifier is unique to the transmitter sub-system and to the sequence of codes.

4. A system according to claim 1, wherein the Wiegand protocol identifier is unique to the transmitter sub-system.

5. A system according to claim 1, wherein the secure access signal is configured to indicate that the secure access signal comprises the Wiegand protocol identifier.

6. A system according to claim 1, wherein the code is encrypted using a key allocated to the transmitter sub-system.

7. A system according to claim 1, said receiver sub-system further comprising means for identifying the sequence of codes based on the Wiegand protocol identifier included in the received secure access signal.

8. A system according to claim 1, said receiver sub-system further comprising means for testing the code included in the received secure access signal to determine if the code is a next code in the sequence of codes.

9. A system according to claim 1, wherein said request is generated based on a button press.

10. A system according to claim 1, wherein said transmitter sub-system comprises a plurality of buttons.

11. A system according to claim 10, wherein each of said buttons has a different associated Wiegand protocol identifier.

12. A system according to claim 1, wherein said request is a biometric signal.

13. A system according to claim 12, further comprising a database comprising one or more biometric signatures.

14. A system according to claim 13, wherein the transmitter sub-system further comprises means for populating said database of biometric signatures.

15. A system according to claim 12, wherein a range of Wiegand protocol identifiers are allocated to the transmitter sub-system.

16. A system according to claim 12, wherein a current Wiegand protocol identifier is changed upon one or more of the biometric signatures in a database associated with the system being erased.

17. A system according to claim 12, wherein the biometric signal is responsive based on one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.

18. A system according to claim 1, wherein the controlled item is one of:

a locking mechanism of a door; and

an electronic lock on a Personal Computer (PC).

19. A transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a receiver sub-system comprising means for

receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal, wherein the transmitter subsystem comprises:

means for storing a Wiegand protocol identifier;

means for receiving a request;

means for generating a code from a sequence of codes based on the Wiegand protocol identifier, upon receiving the request;

means for encoding the code and the Wiegand protocol identifier; and

means for transmitting said secure access signal comprising the code and the encoded Wiegand protocol identifier embedded therein.

20. A transmitter sub-system according to claim 19, wherein the sequence of codes is unique to the transmitter sub-system.

21. A transmitter sub-system according to claim 19, wherein the Wiegand protocol identifier is unique to the transmitter sub-system and to the sequence of codes.

22. A transmitter sub-system according to claim 19, wherein the Wiegand protocol identifier is unique to the transmitter sub-system.

23. A transmitter sub-system according to claim 19, wherein the secure access signal is configured to indicate that the secure access signal comprises the Wiegand protocol identifier.

24. A transmitter sub-system according to claim 19, wherein the code is encoded using a key allocated to the transmitter sub-system.

25. A transmitter sub-system according to claim 19, said receiver sub-system further comprising means for identifying the sequence of codes based on the Wiegand protocol included in the received secure access signal.

26. A transmitter sub-system according to claim 19, said receiver sub-system further comprising means for testing the code included in the received secure access signal to determine if the code is a next code in the sequence of codes.

27. A transmitter sub-system according to claim 19, wherein said request is generated based on a button press.

28. A transmitter sub-system according to claim 19, wherein said transmitter sub-system comprises a plurality of buttons.

29. A transmitter sub-system according to claim 28, wherein each of said buttons has a different associated Wiegand protocol identifier.

30. A transmitter sub-system according to claim 19, wherein said request is a biometric signal.

31. A transmitter sub-system according to claim 30, further comprising a database comprising one or more biometric signatures.

32. A transmitter sub-system according to claim 31, wherein the transmitter sub-system further comprises means for populating said database of biometric signatures.

33. A transmitter sub-system according to claim 30, wherein a range of Wiegand protocol identifiers are allocated to the transmitter sub-system.

34. A transmitter sub-system according to claim 33, wherein a current Wiegand protocol identifier is changed upon one or more of the biometric signatures in a database associated with the system being erased.

35. A transmitter sub-system according to claim 30, wherein the biometric signal is responsive based on one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.

36. A transmitter sub-system according to claim 19, wherein the controlled item is one of:

a locking mechanism of a door; and

an electronic lock on a Personal Computer (PC).

37. A receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on said Wiegand identifier, upon receiving the request, means for encoding the code and the Wiegand identifier, and means for

transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier, wherein the receiver sub-system comprises:

means for receiving the transmitted secure access signal comprising the code and the encoded Wiegand protocol identifier; and

means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier.

38. A method for providing secure access to a controlled item, the method comprising the steps of:

receiving a request;

generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

encoding the code and the Wiegand protocol identifier;

transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier to a controller of said controlled item; and

providing conditional access to the controlled item dependent upon said code and said Wiegand identifier.

39. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to provide secure access to a controlled item, said computer program product comprising:

code for receiving a request;

code for generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

code for encoding the code and the Wiegand protocol identifier;

code for transmitting a secure access signal comprising the code and the Wiegand encoded protocol identifier to a controller of said controlled item, wherein said controller provides conditional access to the controlled item dependent upon said code and said Wiegand identifier.

40. A computer program product having a computer readable medium having a computer program recorded therein for directing a processor to transmit a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a request;

code for generating a code from a sequence of codes based on a Wiegand identifier, upon receiving the request;

code for encoding the code and the Wiegand protocol identifier; and

code for transmitting said secure access signal comprising the code and the encoded Wiegand protocol identifier to a controller of said controlled item, wherein said controller provides conditional access to the controlled item dependent upon said code and said Wiegand identifier.

41. A method of enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier,

and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said method comprising the steps of:

receiving a biometric signal; and

storing a biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and

classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

42. A method according to claim 41, wherein:

if the database of biometric signatures is not empty, and if a predefined succession of finger presses to the biometric sensor are made, the method comprises a further step of:

enrolling one of a further administrator and an ordinary user.

43. An apparatus for enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said apparatus comprising:

receiving means for receiving a biometric signal; and

storage means for storing the biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and

classification means for classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

44. A computer program product having a computer readable medium having a computer program recorded therein for enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising means for storing a Wiegand protocol identifier, means for receiving a request, means for generating a code from a sequence of codes based on the Wiegand identifier, means for encoding the code and the Wiegand protocol identifier, and means for transmitting a secure access signal comprising the code and the encoded Wiegand protocol identifier, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon said code and said Wiegand protocol identifier, said program comprising:

code for receiving a biometric signal representing a biometric signature; and

code for storing the biometric signature in the database, as a representation of the biometric signal, if the database of biometric signatures is empty; and

code for classifying the stored biometric signature as an administrator, thereby enrolling the received biometric signature.

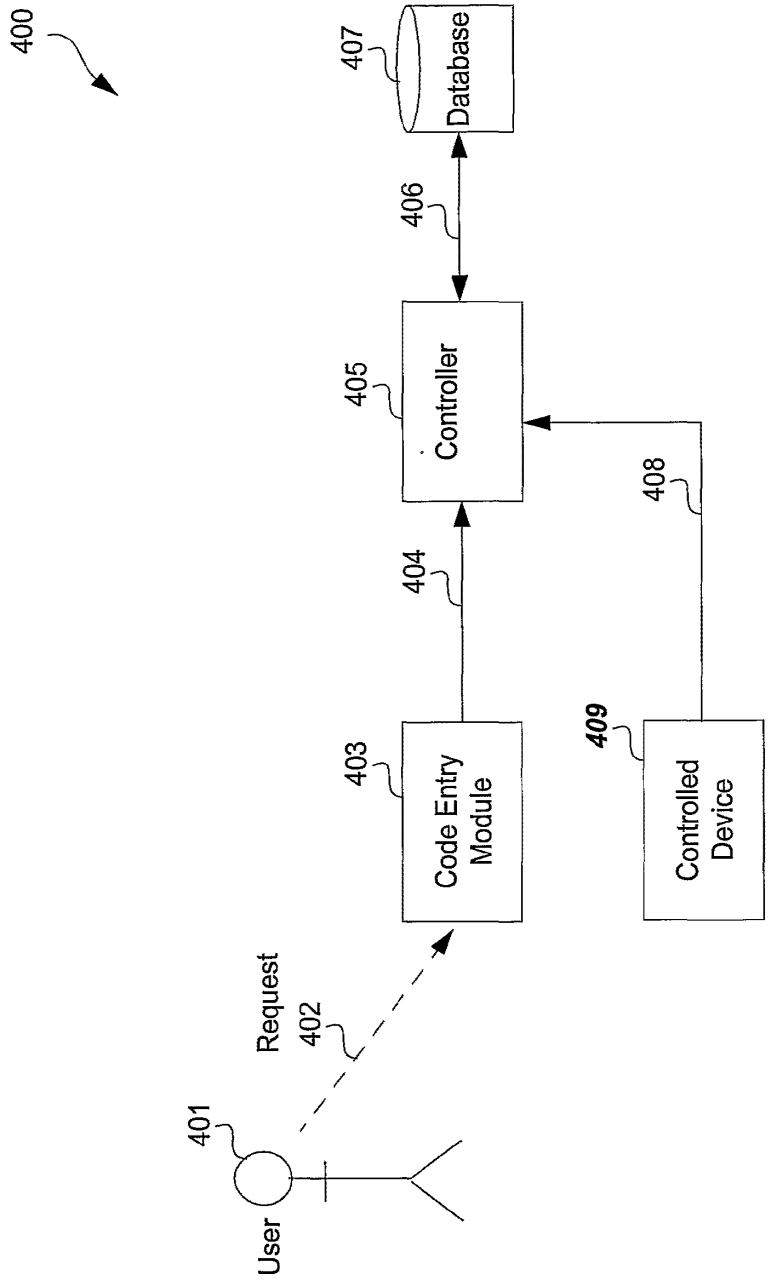


Fig. 1
(prior art)

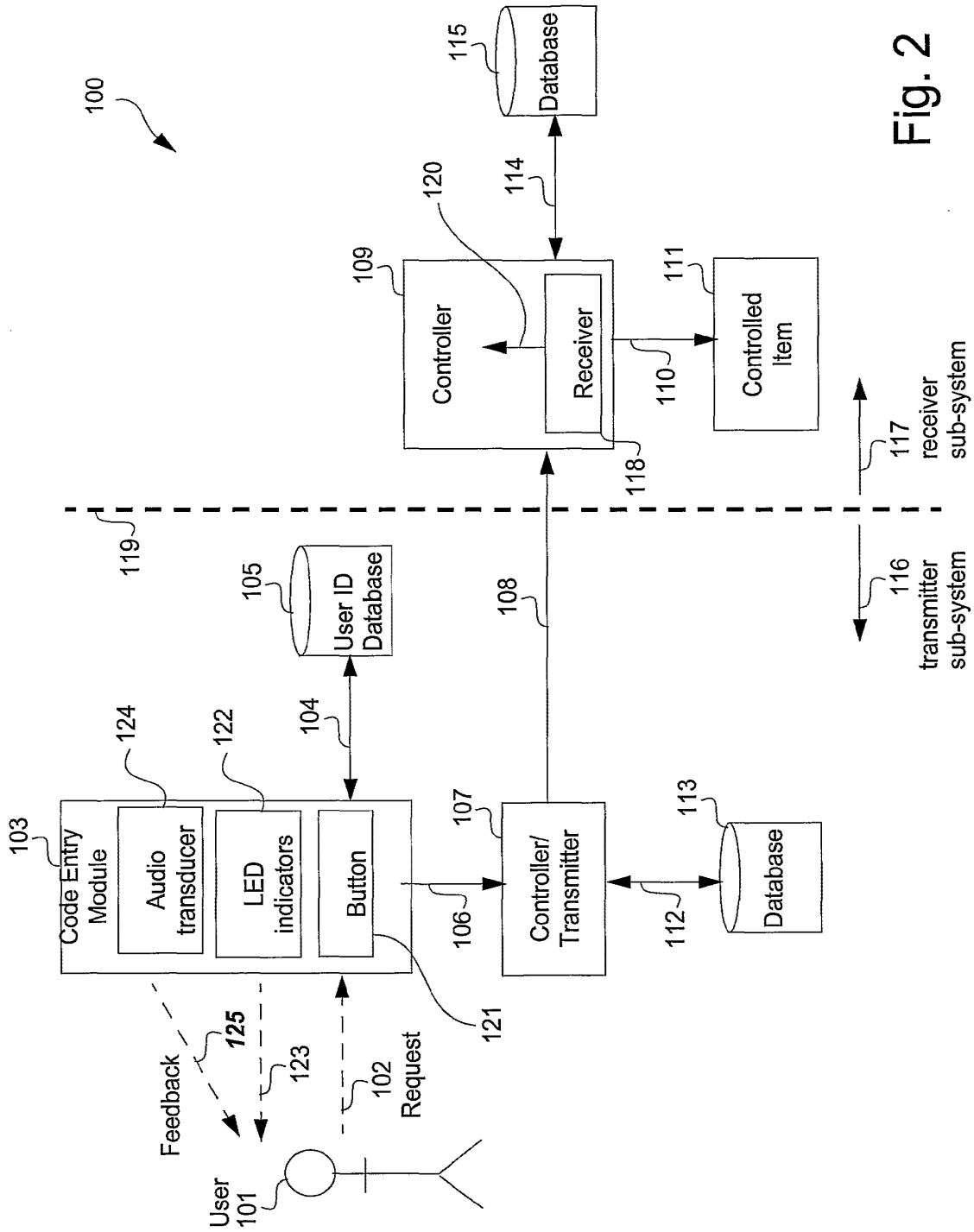

100
115
Database
114
120
109
Controller
Receiver
111
Controlled Item
110
118
117
receiver sub-system
119
116
transmitter sub-system
105
User ID Database
108
124
122
104
103
Code Entry Module
Audio transducer
LED indicators
Button
107
Controller/ Transmitter
113
Database
106
112
121
125
123
102
Feedback
Request
User
101

Fig. 2

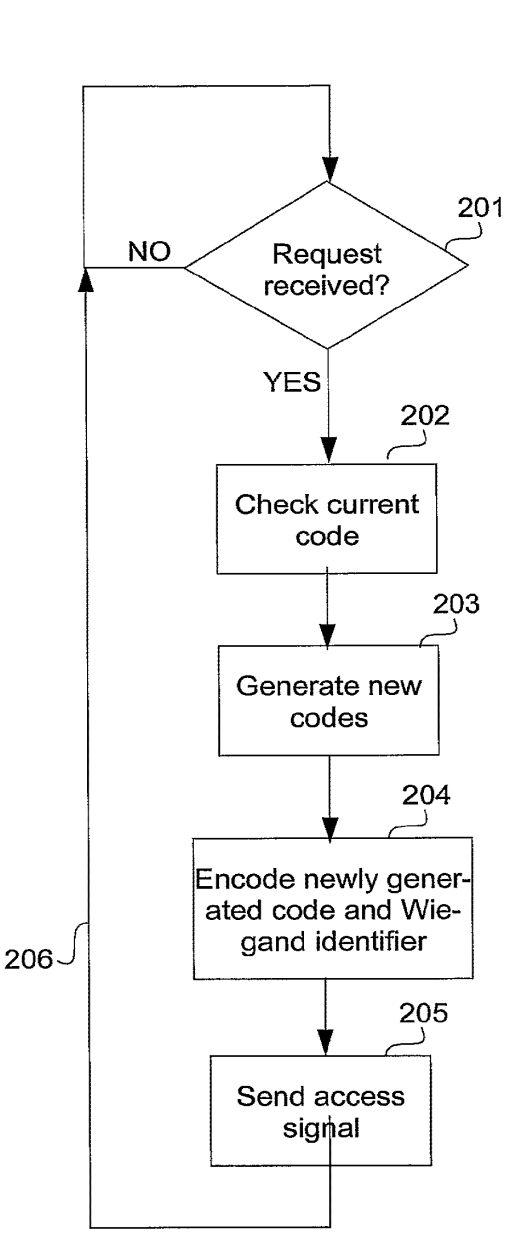
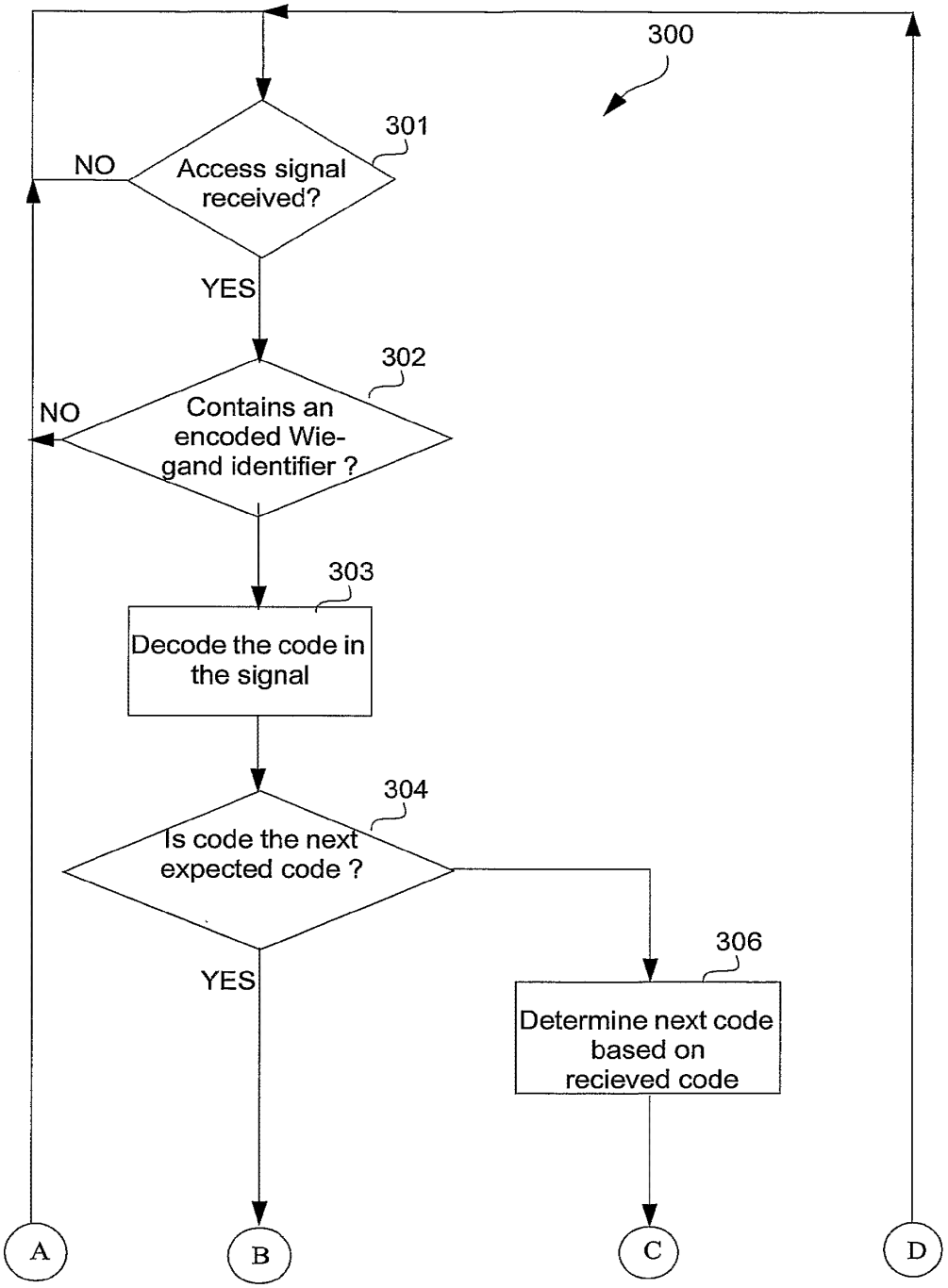

200
201
Request received?
NO
YES
202
Check current code
203
Generate new codes
204
Encode newly generated code and Wiegand identifier
205
Send access signal
206

Fig. 3


300
301
Access signal received?
NO
YES
302
Contains an encoded Wie-gand identifier ?
NO
303
Decode the code in the signal
304
Is code the next expected code ?
YES
306
Determine next code based on recieved code
A
B
C
D

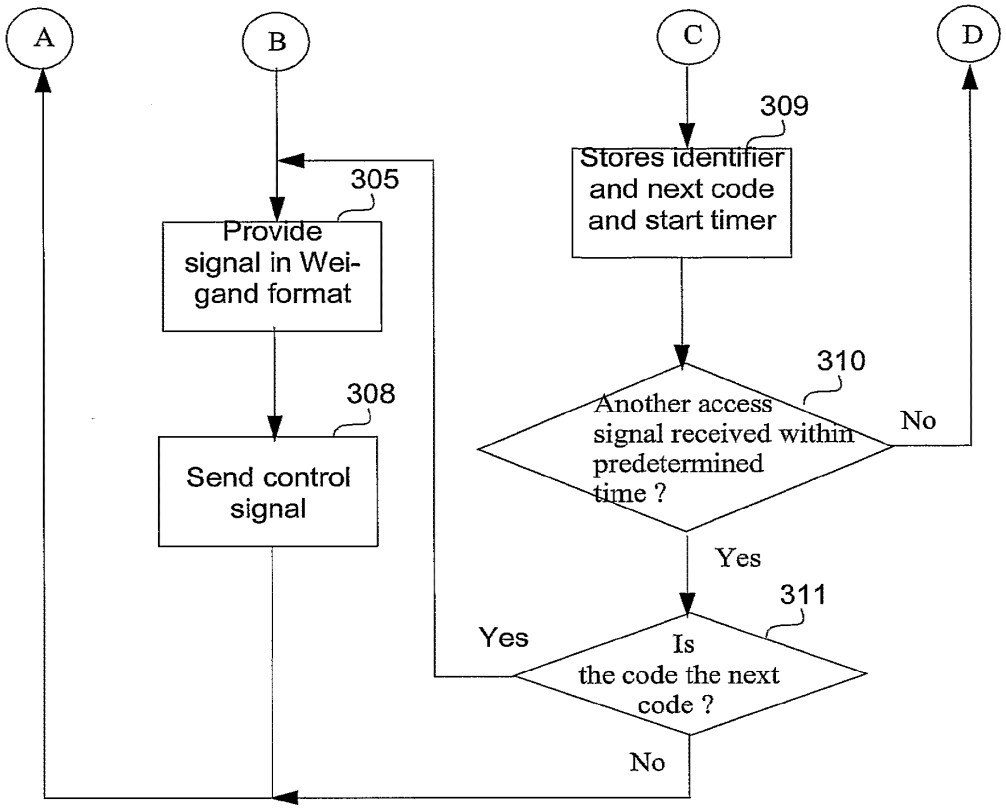

A
B
C
D
309
Stores identifier and next code and start timer
305
Provide signal in Wei-gand format
310
Another access signal received within predetermined time ?
No
308
Send control signal
Yes
311
Yes
Is the code the next code ?
No

Fig. 4[A:B]

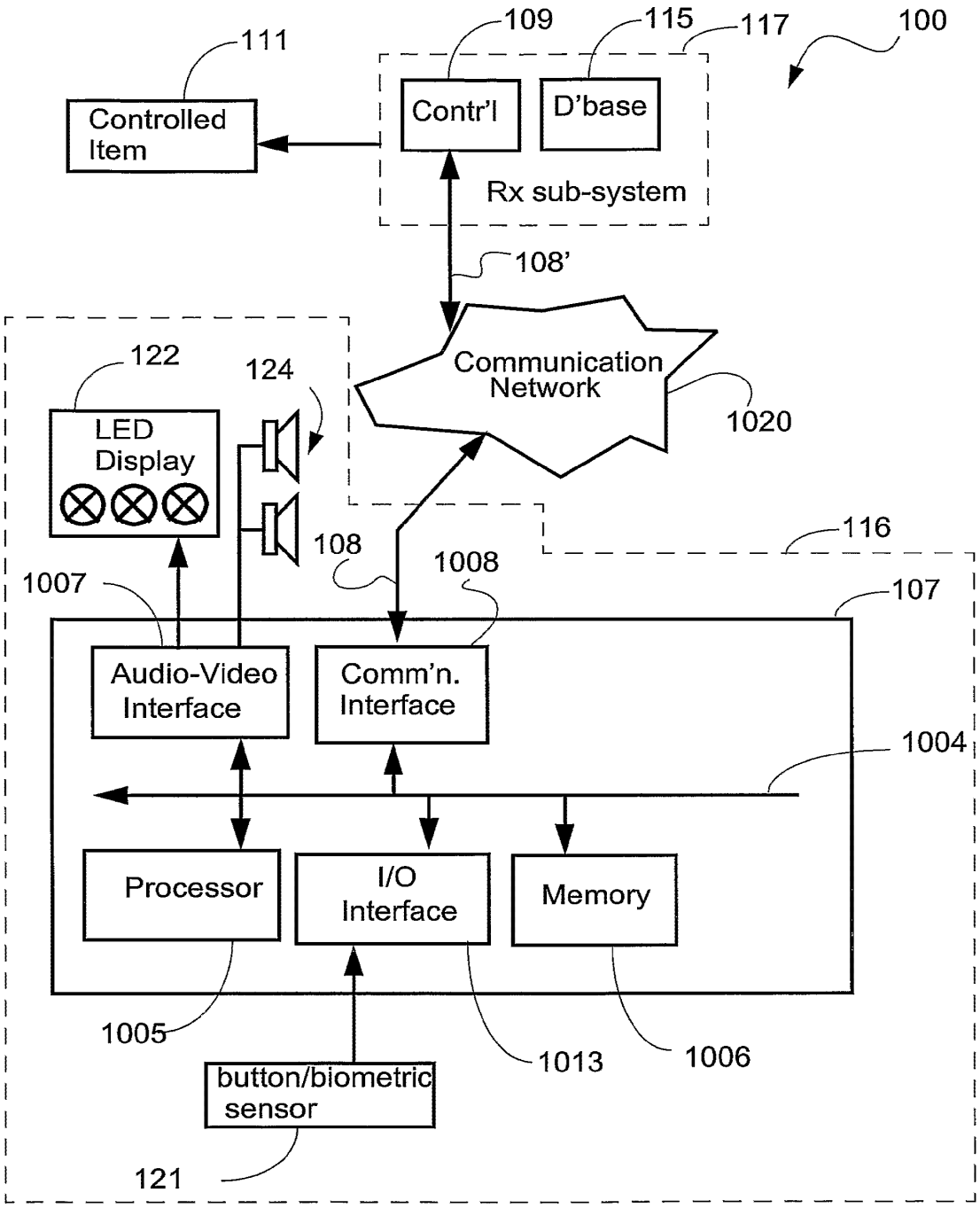

111
109
115
117
100
Controlled Item
Contr'l
D'base
Rx sub-system
108'
Communication Network
1020
122
124
LED Display
108
116
1008
1007
107
Audio-Video Interface
Comm'n. Interface
1004
Processor
I/O Interface
Memory
1005
1013
1006
button/biometric sensor
121

Fig. 5

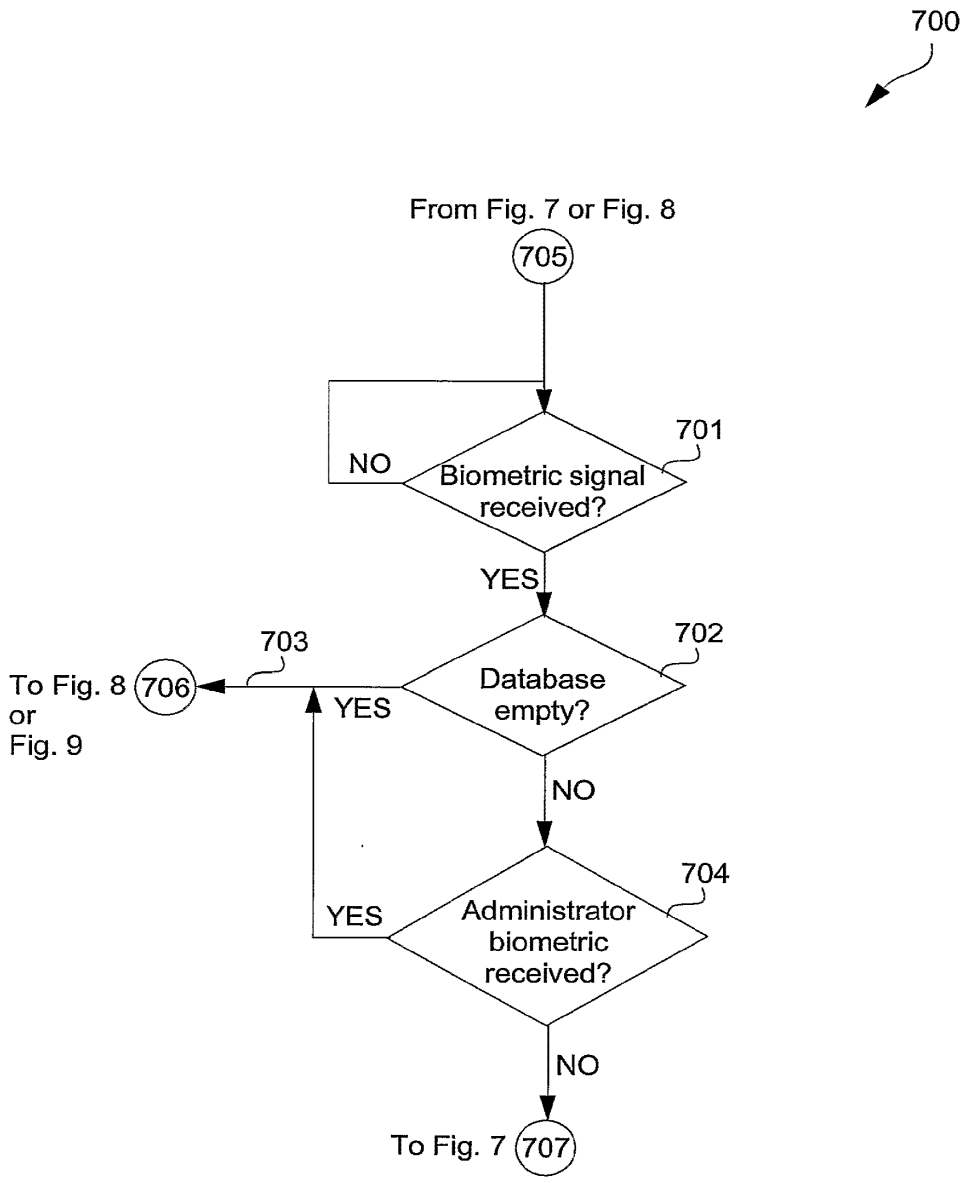
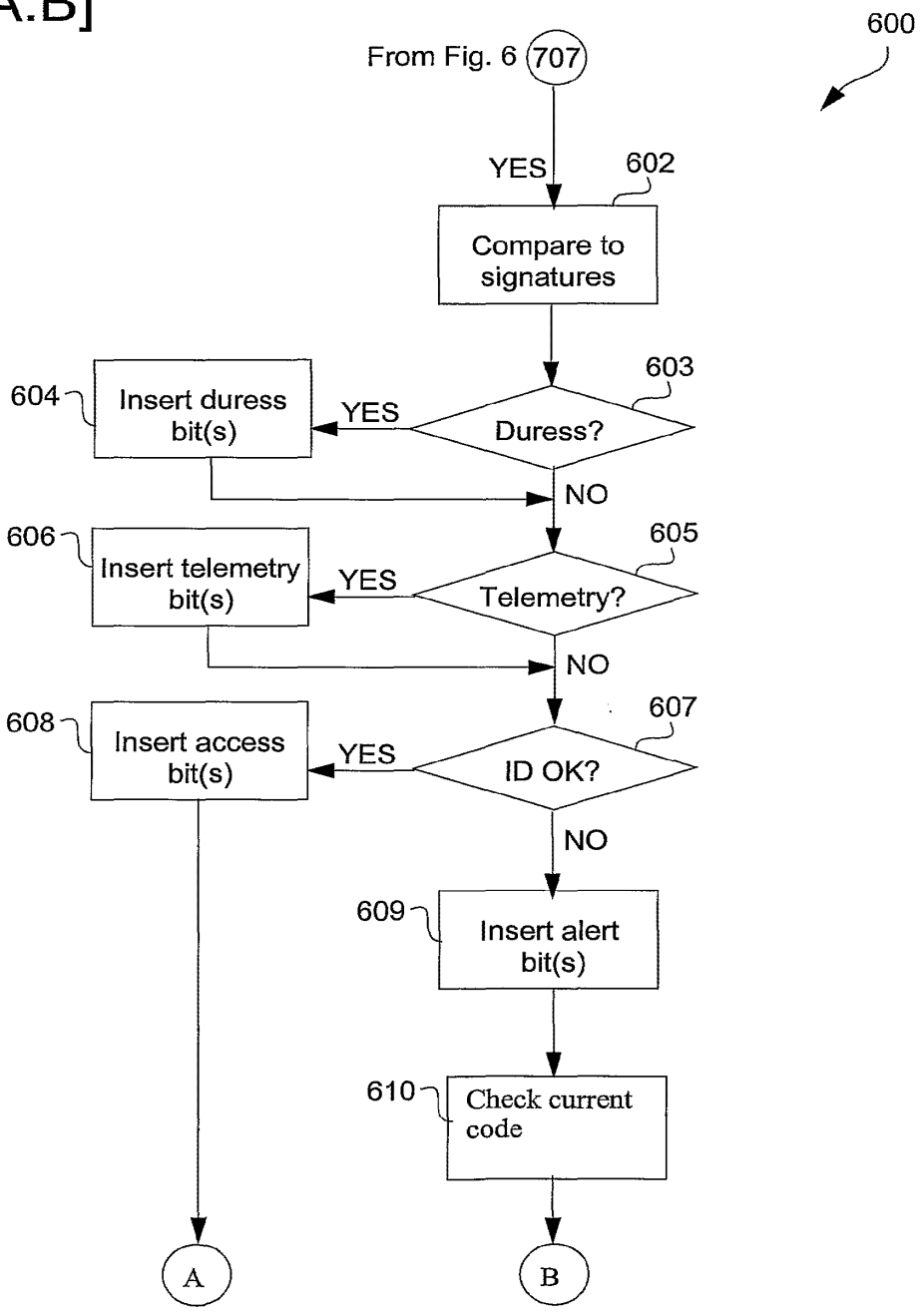

700
From Fig. 7 or Fig. 8
705
701
Biometric signal received?
NO
YES
703
702
To Fig. 8 or Fig. 9
706
Database empty?
YES
NO
704
YES
Administrator biometric received?
NO
To Fig. 7
707

Fig. 6

Fig. 7[A:B]


600
From Fig. 6
707
YES
602
Compare to signatures
603
604
Insert duress bit(s)
YES
Duress?
NO
606
Insert telemetry bit(s)
YES
605
Telemetry?
NO
608
Insert access bit(s)
YES
607
ID OK?
NO
609
Insert alert bit(s)
610
Check current code
A
B

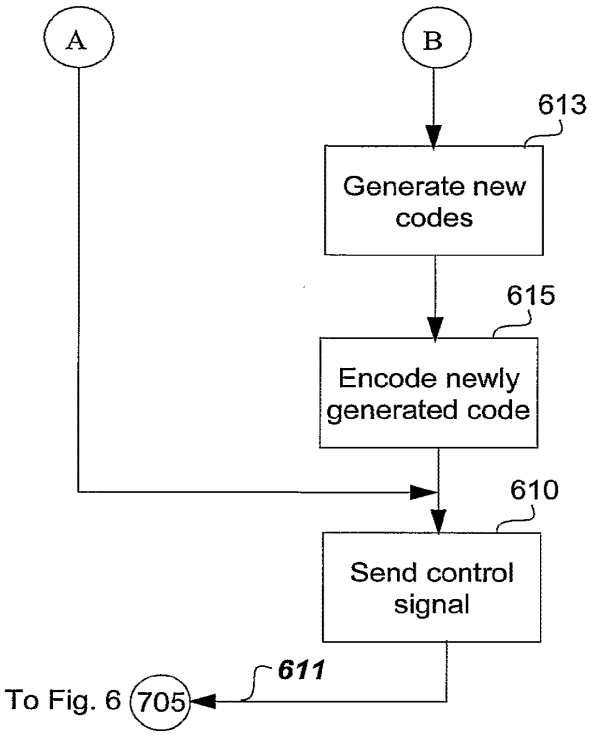

A
B
613
Generate new codes
615
Encode newly generated code
610
Send control signal
611
To Fig. 6
705

Fig. 7[A:B]

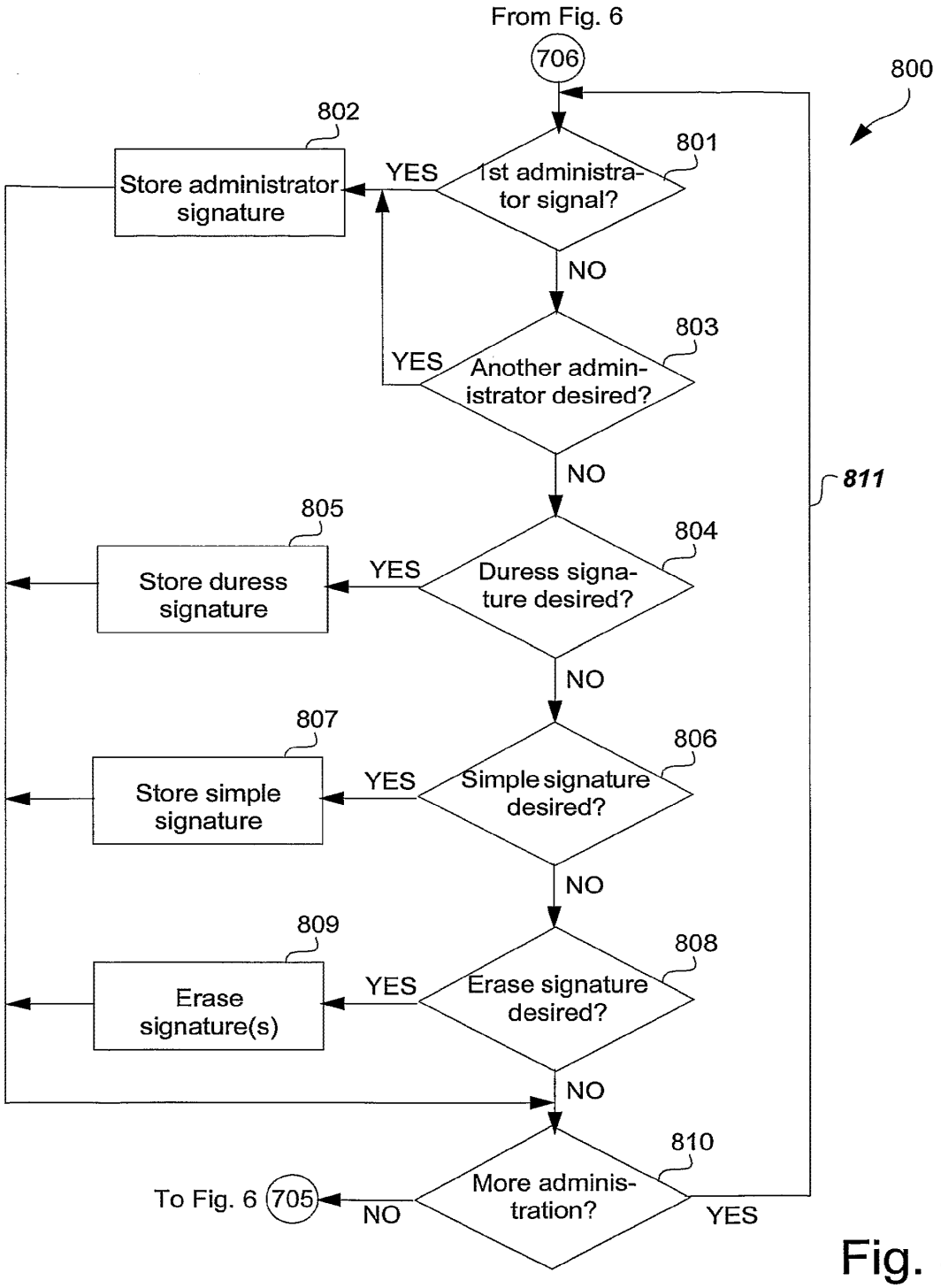

From Fig. 6
706
800
802
801
Store administrator signature
YES
1st administrator signal?
NO
803
YES
Another administrator desired?
NO
811
805
804
Store duress signature
YES
Duress signature desired?
NO
807
806
Store simple signature
YES
Simple signature desired?
NO
809
808
Erase signature(s)
YES
Erase signature desired?
NO
810
To Fig. 6
705
NO
More administration?
YES

Fig. 8

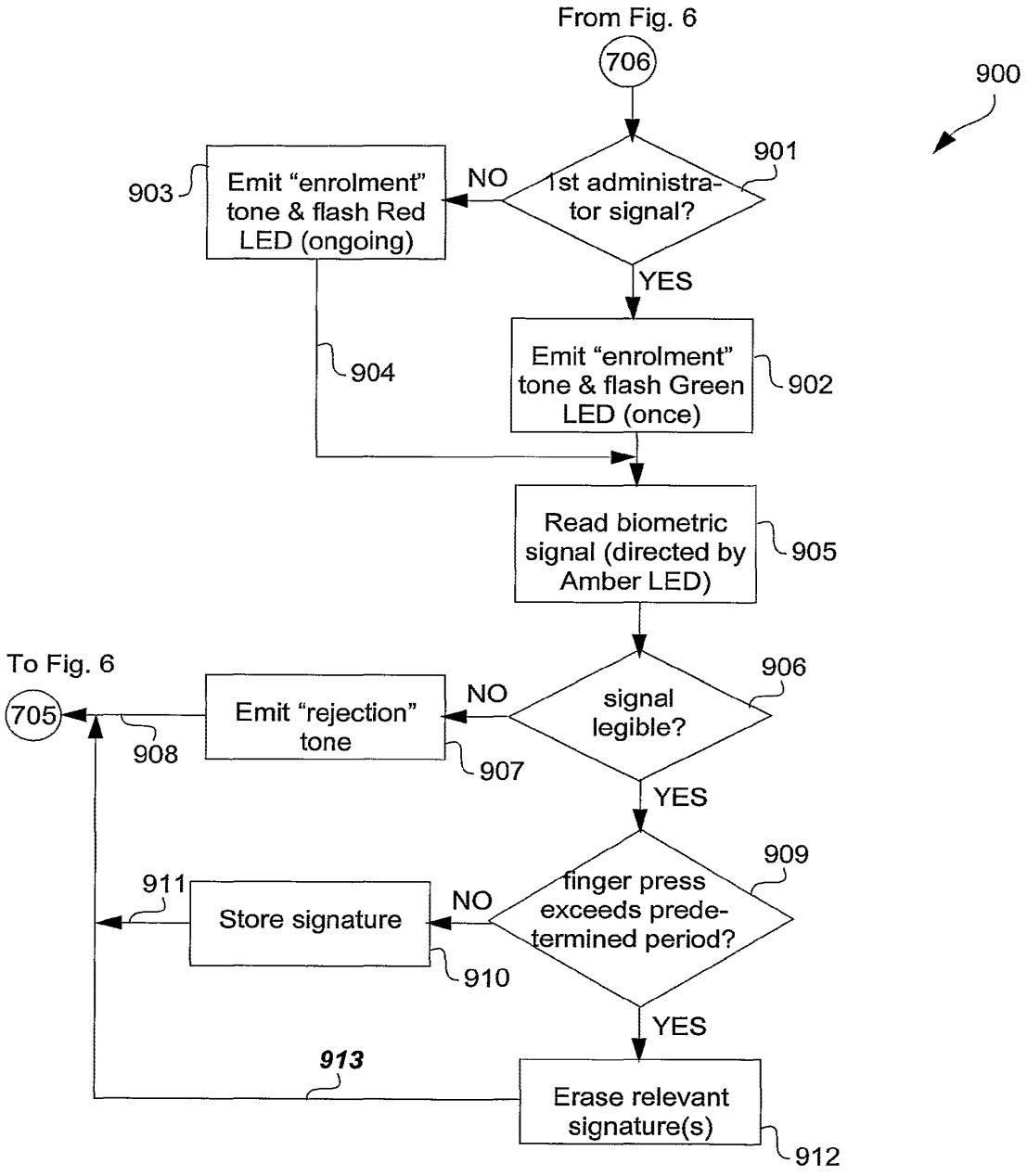

From Fig. 6
706
900
901
1st administrator signal?
NO
903
Emit "enrolment" tone & flash Red LED (ongoing)
YES
904
Emit "enrolment" tone & flash Green LED (once)
902
Read biometric signal (directed by Amber LED)
905
To Fig. 6
705
906
signal legible?
NO
Emit "rejection" tone
908
907
YES
909
finger press exceeds predetermined period?
911
Store signature
NO
910
YES
913
Erase relevant signature(s)
912

Fig. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2007/000311

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 9/32 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPOQUE Internal : TEXTE (access, code, fixed, rolling, Wiegand, Keeloq and like terms)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2005/018137 A1 (SECURICOM (NSW) PTY LTD) 24 February 2005 Abstract, page 2 lines 13-18, page 16 line 18 to page 17 line 24, claim 41, figures	1-40
Y	WO 2004/039119 A1 (ANZON AUTODOOR LIMITED) 6 May 2004 Abstract, figure 2, claims 7-9	1-40
Y	US 6484260 B1 (SCOTT et al.) 19 November 2002 Abstract, column 3 lines 4-19, column 9 lines 38-53, claims	1-40
Y	US 6154544 (FARRIS et al.) 28 November 2000 Abstract, column 2 line 65 to column 3 line 27, claims	1-40

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 May 2007	- 9 MAY 2007
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **DALE SIVER** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : (02) 6283 2196

WAVELYNX EX. 1003, Pg. 1469
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2007/000311

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6882729 B2 (ARLING et al.) 19 April 2005 Column 7 line 1 to column 8 line 67, claim 51	1-40
Y	US 2002/0034303 A1 (FARRIS et al.) 21 March 2002 Whole document, especially paragraphs 10,11,37,38, claims	1-40
P,X	AU 2006203768 A1 (ASSA ABLOY IDENTIFICATION TECH. GROUP AB) Published 15 March 2007 , Priority 31 August 2005	1,19,37,40
Y	US 6956460 B2 (TSUI) 18 October 2005 Whole document	1-40
Y	US 6956495 B2 (KLEIN et al.) 18 October 2005 Abstract, column 1 line 60 to column 2 line 23, column 5 lines 12-62	1-40
A	US 2005/0195066 A1 (VANDRUNEN et al.) 8 September 2005 Abstract, paragraphs 9,26,34,35	1
A	US 6026165 (MARINO et al.) 15 February 2000 Abstract, figure 3	1

WAVELYNX EX. 1003, Pg. 1470
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. PCT/AU2007/000311

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	2005018137	AU	2004301168	CA	2535434	CN	1836399
		EP	1661298				
WO	2004039119	AU	2003267878				
US	6484260	AU	37610/99	GB	2353386	WO	9956429
US	6154544	AU	59213/96	AU	2003265424	BR	9606663
		CA	2193846	CA	2443452	CA	2493715
		EP	0771498	GB	2407901	US	6690796
		US	6810123	US	6980655	US	2002034303
		US	2002191794	US	2003118187	US	2004066936
		US	2004243813	US	2006109978	WO	9637063
		WO	2004017167				
US	6882729	AU	2003259786	CA	2503660	EP	1579626
		US	2004117632	US	2005195979	WO	2004056034
		AU	59213/96	AU	2003265424	BR	9606663
		CA	2193846	CA	2443452	CA	2493715
		EP	0771498	GB	2407901	US	6154544
		US	6690796	US	6810123	US	6980655
		US	2002034303	US	2002191794	US	2003118187
		US	2004066936	US	2004243813	US	2006109978
		WO	9637063	WO	2004017167		
AU	2006203768	CA	2556843	EP	1760985	US	2007046424
US	6956460	AU	2003235585	CA	2507869	US	2003189530
		US	2003193448	US	2006012461	WO	03060850
US	6956495	US	2002175827				
US	2005195066	AU	2005222330	CA	2558398	EP	1725994
		US	7193502	WO	2005088562		
US	6026165	US	6167137				

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX

WAVELYNX EX. 1003, Pg. 1471
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2432
Michael Davis	)	Confirmation No.: 9292
Serial No.: 12/539,431	)	Examiner: Cordelia P.K. Zecher
Filed: August 11, 2009	)	SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Atty. File No.: 2943-178	)	*Electronically Submitted*
Entitled: "Secure Wiegand Communications"	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references cited on attached Form(s) PTO/SB08a and PTO/SB08b are being called to the attention of the Examiner.

☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.

☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.

☐ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).

☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.

☐ To the best of applicants' belief, the pertinence of the foreign-language references is believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.

☐ Examiner's attention is drawn to the following related applications:

Serial No. _____ filed _____ (Attorney Ref. No. _____)

Serial No. _____ filed _____ (Attorney Ref. No. _____)

☐ Other:_____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be drawn as to the pertinence

WAVELYNX EX. 1003, Pg. 1472
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

☒	**37 CFR 1.97(b)**: No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction): ☐ Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or ☐ Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application, or ☒ Before the mailing date of a first Office Action on the merits, or ☐ Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114. Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.
☐	**37 CFR 1.97(c)**: The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of any one of the following conditions: (1) a final action under 37 C.F.R. 1.113, or (2) a notice of allowance under 37 C.F.R. 1.311, or (3) an action that otherwise closes prosecution in the application. This Information Disclosure Statement is accompanied by: ☐ A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970. OR ☐ Please charge Deposit Account 19-1970 in the amount of $180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.
☐	**37 CFR 1.97(d)**: This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c). ☐ This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e) AND ☐ Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of $180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.

WAVELYNX EX. 1003, Pg. 1473
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

☐ The undersigned certifies that:

☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).

☐ A copy of the communication from the foreign patent office is enclosed.

OR

☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: _____

Matthew R. Ellsworth
Registration No. 56345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: February 7, 2012

WAVELYNX EX. 1003, Pg. 1474
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2432
	)	
GUTHERY et al.	)	Examiner: ZECHER, CORDELIA P K
	)	
Serial No.: 12/539,431	)	Confirmation No.: 9292
	)	
Filed: August 11, 2009	)	RESPONSE TO RESTRICTION REQUIREMENT
	)	
Atty. File No.: 2943AAAB-178	)	
	)	
For: "SECURE WIEGAND COMMUNICATIONS"	)	***Filed Electronically***
	)	
	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Response to Restriction Requirement is submitted in reply to the Examiner's Action having a mailing date of January 26, 2012, in connection with the above-identified patent application. Although no fees are believed due in connection with the filing of this paper, please charge any fees deemed necessary to Deposit Account No. 19-1970.

In the Office Action dated January 26, 2012, a requirement that one of three identified claim groups be selected for examination is set forth. In response to the Restriction Requirement, Applicants hereby elect the claims in Group I (Claims 1-29), identified by the Office Action as being drawn to obfuscating data using a rolling code, for immediate prosecution on the merits.

Applicants hereby expressly reserve the right to file divisional applications directed to the non-elected claims of Group II (Claims 30-36) and Group III (Claims 37-40), without the need to file a terminal disclaimer.

The Examiner is invited to contact the undersigned by telephone if the Examiner believes that doing so would expedite the resolution of this case.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Registration No. 56,345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: February 27, 2012

WAVELYNX EX. 1003, Pg. 1476
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Electronic Acknowledgement Receipt	
EFS ID:	12167200
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943-178
Receipt Date:	27-FEB-2012
Filing Date:	11-AUG-2009
Time Stamp:	15:45:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response to Election / Restriction Filed	RESPONSE_RESTRICTION_REQUIREMENT.pdf	84395 17eb56ad1c4daba7cf9e79b9a9391324f26d43fa	no	2

Warnings:
Information:

Total Files Size (in bytes):	84395

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/539,431	08/11/2009	Michael Davis	2943AAAB-178	9292

22442 7590 04/13/2012

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER	
ZECHER, CORDELIA P K	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
04/13/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

WAVELYNX EX. 1003, Pg. 1479
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Office Action Summary	Application No.	Applicant(s)	
	12/539,431	DAVIS ET AL.	
	Examiner	Art Unit	
	CORDELIA ZECHER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2012*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-29* is/are pending in the application.

5a) Of the above claim(s) *30-40* is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-29* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☒ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *11 August 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

WAVELYNX EX. 1003, Pg. 1480
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

DETAILED ACTION

Election/Restrictions

1. Applicant's election of Group I in the reply filed on February 27, 2012 is acknowledged. Because applicant did not distinctly and specifically point out the supposed errors in the restriction requirement, the election has been treated as an election without traverse (MPEP § 818.03(a)).

Information Disclosure Statement

2. It is noted that the number of references that have been filed in the various Information Disclosure Statements is quite extensive. The information has only been considered by verifying the presence of the documents, and a cursory review of them.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. The term "human perceivable amount of time" in claim 11 is a relative term which renders the claim indefinite. The term "human perceivable amount of time" is not defined by the claim, the specification does not provide a standard for ascertaining the

requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1 – 3, 7, 16, 19, 20 and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Hardacker et al's US Publication 2009/0128392 A1.

7. Referring to claim 1, Hardacker teaches:

a. Obfuscating data transmitted in a first message from a first communication device to a second communication device, wherein the first and second communication devices communicate using a unidirectional communication protocol (paragraph 54) and wherein the obfuscation of the data is effected with a predetermined code (paragraphs 45 and 50).

3. Referring to claim 2, Hardacker teaches the predetermined code is agreed upon between the first and second communication devices prior to obfuscation of the data in the first message (paragraph 45).

4. Referring to claims 3 and 20, Hardacker teaches the predetermined code is one of a plurality of codes within a rolling code sequence, wherein the first and second communication devices each have a copy of the rolling code sequence and wherein data communicated between the first and second communication devices subsequent

to the first message is obfuscated with a code from the rolling code sequence that is different from the predetermined code (paragraph 43).

5. Referring to claims 7 and 22, Hardacker teaches obfuscation comprises computing an XOR of the predetermined code and the data (paragraphs 26, 28 and 57).

6. Referring to claim 16, Hardacker teaches control signals are used to accommodate bi-directional communications in one of a half-duplex configuration and a full-duplex configuration (paragraph 54).

7. Referring to claim 19, Hardacker teaches:

b. A rolling code generator operable to generate a plurality of distinct rolling codes (paragraph 52).

c. A message formatting engine, wherein the message formatting engine is operable to retrieve a first rolling code from the rolling code generator and obfuscate data with the first rolling code prior to transmitting the data to an upstream device (paragraph 57).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

10. Claims 4 – 6, 8, 21 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardacker as applied above, and further in view of Davis US Publication 2007/0046424 A1.

11. Referring to claims 4, 5 and 21, Hardacker discloses all of the limitations of the parent claim. Hardacker does not explicitly disclose the Wiegand protocol. However, Davis discloses the Wiegand protocol is used for unidirectional communication and is an industry standard (paragraphs 8 and 9). Hardacker and Davis are analogous art because they are from the same field of endeavor, secure communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hardacker and Davis before him or her, to modify the unidirectional communication of Hardacker to include the Wiegand protocol of Davis. The suggestion/motivation for doing so would have been because Wiegand is an industry standard and is used for unidirectional communications (paragraphs 8 and 9).

12. Referring to claim 6, Davis teaches the Wiegand message is encapsulated in a TCP packet and is transmitted over an IP network from the first communication device to the second communication device (paragraph 36). At the time of the invention, it

would have been obvious to one of ordinary skill in the art, having the teachings of Hardacker and Davis before him or her, to modify the communication of Hardacker to include the TCP/IP protocol of Davis. The suggestion/motivation for doing so would have been because TCP/IP is a known communication protocol.

13. Referring to claims 8 and 23, Davis the predetermined code is employed to identify an authenticity of the first communication device (paragraph 23) and a timestamp (claim 19). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hardacker and Davis before him or her, to modify the rolling code of Hardacker to include the timestamp and identity verification of Davis. The suggestion/motivation for doing so would have been because rolling codes can be used for authentication (paragraph 23) and a timestamp is used to indicate when a message was generated so as to be used for the authentication (paragraph 14).

14. Claims 9 – 14, and 24 – 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardacker as applied above, and further in view of Davis et al's US Publication 2006/0123466 A1.

15. Referring to claims 9 and 24, Hardacker discloses all the limitations of the parent claim. Hardacker does not explicitly disclose receiving a message from the first device and then transitioning to a second mode. However, Davis teaches:

a. Receiving a message at the first communication device (paragraph 33)

b. Determining that the message received at the first communication device was transmitted by the second communication device, wherein determining is performed by one or more of (i) analyzing an out-of-band communication received at the first communication device from the second communication device and (ii) analyzing a special code that identifies the second communication device is an advanced communication device in an advanced communication mode (paragraph 32 and corresponding table).

c. Based on determining that the message was transmitted by the second communication device, transitioning the first communication device from a first mode of operation to a second mode of operation (paragraph 33).

16. Hardacker and Davis are analogous art because they are from the same field of endeavor, secure communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hardacker and Davis before him or her, to modify the unidirectional communication of Hardacker to include the Wiegand communication, including extended protocol of Davis. The suggestion/motivation for doing so would have been to extend the functionality so that improved readers and panels may be implemented (paragraph 5).

17. Referring to claims 10 and 25, Davis teaches the message transmitted by the second communication device comprises an alteration of a control line signal between the first and second communication devices for a predetermined amount of time (paragraphs 32-33).

18. Referring to claims 11 and 26 Davis teaches the predetermined amount of time is less than a human-perceivable amount of time (paragraphs 32-33, table).

19. Referring to claims 12 and 27, Davis teaches the first mode comprises a non-secure Wiegand mode and the second mode comprises a secure Wiegand mode (paragraph 33).

20. Referring to claims 13 and 28, Davis teaches the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode (paragraphs 32 and 33).

21. Referring to claims 14 and 29, Hardacker discloses all the limitations of the parent claim. Hardacker does not explicitly disclose detecting message collision and initiating a cooperative transmission in response to a detected collision. However, Davis discloses in Wiegand communications with multiple readers can result in multiple generators attempting to talk at the same time and creating a collision, and in such an event a rebroadcast message will be sent out one-by-one to each active generator (paragraph 30). Hardacker and Davis are analogous art because they are from the same field of endeavor, secure communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hardacker and Davis before him or her, to modify the unidirectional communication of Hardacker to include the Wiegand communication, including collisions of Davis. The suggestion/motivation for doing so would have been because Wiegand is a protocol that has been in use for many years for unidirectional communication (paragraphs 3 and 4),

and because in Wiegand communications with multiple generators, collision is a known problem (paragraph 30).

22. **Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hardacker as applied above, and further in view of Ngo et al's US Publication 2008/0037466 A1.**

23. Hardacker discloses all of the limitations of the parent claim. Hardacker does not explicitly disclose out-of-band communications are transmitted from the second device to the first device at a timing different from message timing used in the unidirectional protocol. However, Ngo discloses the acknowledgement messages are sent out of band on another channel outside the 60 GHz frequency (paragraph 84). Hardacker and Ngo are analogous art because they are from the same field of endeavor, wireless communication. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hardacker and Ngo before him or her, to modify the acknowledgement messages of Hardacker to include the out of band messaging of Ngo. The suggestion/motivation for doing so would have been so that the acknowledgement is transmitted on a different channel than regular communication (paragraph 84).

24. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardacker as applied above, and further in view of Zhu et al's US Publication 2006/0210081 A1.

25. Referring to claim 17, Hardacker discloses all of the limitations of the parent claim. Hardacker does not explicitly disclose using a stream cipher for encryption. However, Zhu discloses a stream cipher as a conventional encryption method (paragraph 14). Hardacker and Zhu are analogous art because they are from the same field of endeavor, data protection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hardacker and Zhu before him or her, to modify the XOR encryption of Hardacker to include the stream cipher of Zhu. The suggestion/motivation for doing so would have been because stream cipher is a conventional encryption method using XOR (paragraphs 14 and 18).

26. Referring to claim 18, Zhu teaches the first message maintains the same size before and after being obfuscated in the encryption operation (paragraph 28). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Hardacker and Zhu before him or her, to modify the XOR encryption of Hardacker to include the stream cipher of Zhu. The suggestion/motivation for doing so would have been because stream cipher is a conventional encryption method using XOR (paragraphs 14 and 18).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA ZECHER whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CORDELIA ZECHER/
Primary Examiner, Art Unit 2432

Notice of References Cited	Application/Control No. 12/539,431	Applicant(s)/Patent Under Reexamination DAVIS ET AL.	
	Examiner CORDELIA ZECHER	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0123466 A1	06-2006	Davis et al.	726/002
*	B	US-2006/0210081 A1	09-2006	Zhu et al.	380/277
*	C	US-2007/0046424 A1	03-2007	Davis et al.	340/005.8
*	D	US-2008/0037466 A1	02-2008	Ngo et al.	370/329
*	E	US-2009/0128392 A1	05-2009	Hardacker et al.	341/175
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

WAVELYNX EX. 1003, Pg. 1491
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Gilberto Barron Jr.
Sheet	1	of	1	Attorney Docket Number	2943-178

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-kind Code [2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)		
Examiner Initials*	Cite No.[1]	
/C.Z./	1	International Preliminary Report on Patentability for International (PCT) Patent Application No. PCT/US09/53430, mailed Feb. 24, 2011 (Attorney Ref. No. 2943-178-PCT)

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Gilberto Barron Jr.
Sheet	1	of	1	Attorney Docket Number	2943-178

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-kind Code [2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	5696909	12/9/1997	Wallner	
	2	2007/0109101	5/17/2007	Colby	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)		
Examiner Initials*	Cite No.[1]	
	3	ANASHIN "Non-Archimedean Ergodoci Theory and Pseudorandom Generators," Oct. 07, 2007, 39 pages, available at http://arxiv.org/abs/0710.1418v1
	4	BARKER, Cryptanalysis of Shift-Register Generated Stream Cipher Systems, Cryptographic Series No. 39, Aegean Park Press, 1984, Chapters 1-3, pages 1-38
	5	BLUM, M. et al., "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits," SIAM Journal on Computing, Nov. 1984, Vol. 13, No. 4, pp. 850-864.
	6	KOBLITZ, N., p-Adic Number, p-Adic Analysis and Zeta Functions, Chapter 3, Building up Ω, Springer, New York, (1977), pages 52-74.
	7	KUIPERS, et al., Uniform Distribution of Sequences, John Wiley & Sons (1974), 400 pages (Submitted in 3 Parts)
	8	LUBY, M., Pseudorandomness and Cryptographic Applications, Princeton University Press (1996), pages ix-55

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	2943-178

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-kind Code [2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	5600324	2/4/1997	Reed et al.	
	2	5844990	12/1/1998	Kokubu et al.	
	3	6078888	6/20/2000	Johnson, Jr.	
	4	6181252	1/30/2001	Nakano	
	5	6249866	6/19/2001	Brundrett et al.	
	6	6411199	6/25/2002	Geiszler et al.	
	7	6724296	4/20/2004	Hikita et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)		
Examiner Initials*	Cite No.[1]	

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12539431	DAVIS ET AL.
	Examiner	**Art Unit**
	CORDELIA ZECHER	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/09/2012								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	N								
	31	N								
	32	N								
	33	N								
	34	N								
	35	N								
	36	N								

WAVELYNX EX. 1003, Pg. 1495
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12539431	DAVIS ET AL.
	Examiner	**Art Unit**
	CORDELIA ZECHER	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/09/2012								
	37	N								
	38	N								
	39	N								
	40	N								

WAVELYNX EX. 1003, Pg. 1496
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12539431	DAVIS ET AL.
	Examiner	Art Unit
	CORDELIA ZECHER	2432

SEARCHED			
Class	Subclass	Date	Examiner
380	260	4/9/12	cz

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Search	4/9/12	cz
Searched EAST (see attached)	4/9/12	cz

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

WAVELYNX EX. 1003, Pg. 1497
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	8	Attorney Docket Number	2943-178

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-kind Code [2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	3694757	9/26/1972	Hanna, Jr.	
	2	4087626	5/2/1978	Brader	
	3	5187676	2/16/1993	DeVane	
	4	5193115	3/9/1993	Vobach	
	5	5258936	11/2/1993	Gallup et al.	
	6	5357528	10/18/1994	Alon et al.	
	7	5420928	5/30/1995	Aiello et al.	
	8	5446683	8/29/1995	Mullen et al.	
	9	5533128	7/2/1996	Vobach	
	10	5541996	7/30/1996	Ridenour	
	11	5577124	11/19/1996	Anshel et al.	
	12	5608801	3/4/1997	Aiello et al.	
	13	5680131	10/21/1997	Utz	
	14	5686904	11/11/1997	Bruwer	
	15	5751808	5/12/1998	Anshel et al.	
	16	5754603	5/19/1998	Thomas et al.	
	17	5802176	9/1/1998	Audebert	
	18	5825882	10/20/1998	Kowalski et al.	
	19	6044388	3/28/2000	DeBellis et al.	
	20	6052786	4/18/2000	Tsuchida	
	21	6079018	6/20/2000	Hardy et al.	
	22	6097307	8/1/2000	Utz	
	23	6154544	11/28/2000	Farris et al.	
	24	6285761	9/4/2001	Patel et al.	
	25	6314440	11/6/2001	O'Toole et al.	
	26	6487176	11/26/2002	Lehmann	
	27	6542608	4/1/2003	Scheidt et al.	
	28	6606386	8/12/2003	Scheidt et al.	
	29	6608901	8/19/2003	Scheidt et al.	
	30	6691141	2/10/2004	Schmidt	
	31	6718038	4/6/2004	Cusmario	
	32	6810123	10/26/2004	Farris et al.	

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Complete if Known	
Application Number	12/539,431
Filing Date	August 11, 2009
First Named Inventor	Scott B. Guthery
Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	2943-178

Sheet 2 of 8

	33	6885747	4/26/2005	Scheidt et al.	
	34	6931533	8/16/2005	Roberts	
	35	6944768	9/13/2005	Siegel et al.	
	36	6947560	9/20/2005	Smeets et al.	
	37	6988203	1/17/2006	Davis et al.	S
	38	7016925	3/21/2006	Schmidt	
	39	7064665	6/20/2006	Woodall et al.	
	40	7085791	8/1/2006	Barry et al.	
	41	7118033	10/10/2006	Merkert	
	42	7120696	10/10/2006	Au et al.	
	43	7170997	1/30/2007	Petersen et al.	
	44	7190787	3/13/2007	Graunke et al.	
	45	7212632	5/1/2007	Scheidt et al.	
	46	7219113	5/15/2007	Bonaccio et al.	
	47	7277543	10/2/2007	Driscoll	
	48	7293698	11/13/2007	Cheng et al.	
	49	7412056	8/12/2008	Farris et al.	
	50	7492898	2/17/2009	Farris et al.	
	51	7492905	2/17/2009	Fitzgibbon	
	52	2001/0041593	11/15/2001	Asada	
	53	2001/0056534	12/27/2001	Roberts	
	54	2002/0016913	2/7/2002	Wheeler et al.	
	55	2002/0184539	12/5/2002	Fukuda et al.	
	56	2003/0014646	1/16/2003	Buddhikot et al.	
	57	2003/0074319	4/17/2003	Jaquette	
	58	2003/0204541	10/30/2003	Shackleford et al.	
	59	2003/0208697	11/6/2003	Gardner	
	60	2004/0153291	8/5/2004	Kocarev et al.	
	61	2004/0162863	8/19/2004	Barry et al.	
	62	2004/0162864	8/19/2004	Nowshadi et al.	
	63	2005/0002533	1/6/2005	Langin-Hooper et al.	
	64	2005/0010624	1/13/2005	Stehle	
	65	2005/0044119	2/24/2005	Langin-Hooper et al.	
	66	2005/0110210	5/26/2005	Soltys et al.	
	67	2005/0129247	6/16/2005	Gammel et al.	
	68	2005/0166040	7/28/2005	Walmsley	

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Complete if Known	
Application Number	12/539,431
Filing Date	August 11, 2009
First Named Inventor	Scott B. Guthery
Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	2943-178

Sheet	3	of	8

	69	2005/0182946	8/18/2005	Shatford	
	70	2005/0265546	12/1/2005	Suzuki	
	71	2006/0083228	4/20/2006	Ong et al.	
	72	2006/0123466	6/8/2006	Davis et al.	
	73	2006/0174184	8/3/2006	Stroud et al.	
	74	2006/0177056	8/10/2006	Rostin et al.	
	75	2006/0179094	8/10/2006	Onaya et al.	
	76	2006/0206554	9/14/2006	Lauter et al.	
	77	2006/0294312	12/28/2006	Walmsley	
	78	2007/0121943	5/31/2007	Dellow et al.	
	79	2007/0016942	1/18/2007	Sakai et al.	
	80	2007/0034691	2/15/2007	Davis et al.	
	81	2007/0043954	2/22/2007	Fox	
	82	2007/0046424	3/1/2007	Davis et al.	
	83	2007/0057057	3/15/2007	Andresky et al.	
	84	2007/0076864	4/5/2007	Hwang	
	85	2007/0099597	5/3/2007	Arkko et al.	
	86	2007/0165847	7/19/2007	Langin-Hooper et al.	
	87	2007/0165848	7/19/2007	Reyes	
	88	2007/0178886	8/2/2007	Wang et al.	
	89	2007/0183593	8/9/2007	Yoshida et al.	
	90	2007/0195952	8/23/2007	Singanamala	
	91	2007/0214293	9/13/2007	Gangstoe et al.	
	92	2007/0269048	11/22/2007	Hsu	
	93	2007/0293192	12/20/2007	De Groot	
	94	2007/0294528	12/20/2007	Shoji et al.	
	95	2007/0294531	12/20/2007	Alten	
	96	2007/0294539	12/20/2007	Shulman et al.	
	97	2007/0296817	12/27/2007	Ebrahimi et al.	
	98	2008/0001778	1/3/2008	Challener et al.	
	99	2008/0046493	2/21/2008	Rosenberg	
	100	2008/0005532	1/3/2008	Liao et al.	
	101	2008/0061941	3/13/2008	Fischer et al.	
	102	2008/0010218	1/10/2008	Zank	
	103	2008/0012690	1/17/2008	Friedrich	
	104	2008/0016363	1/17/2008	Lapstun et al.	

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	4	of	8	Attorney Docket Number	2943-178

	105	2008/0184349	7/31/2008	Ting	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	106	AU 2006203768	3/15/07	Davis et al.		
	107	CA 2556843	2/28/07	Davis et al.		
	108	WO 01/013218	02/22/01	Siemens Aktiengesellschaft		(Translated Abstract Attached)
	109	WO 01/18331	03/15/01	Electec System Aktiebolag		
	110	WO 03/027832	04/03/03	Intel Corporation		
	111	WO 03/042812	05/22/03	Everbee Networks		(Translated Abstract Attached)
	112	WO 04/010373	01/29/04	Banque-Tec International Pty Ltd		
	113	WO 05/001777	01/06/05	SCM Microsystems GMBH		
	114	WO 2004/039119	05/06/04	Anzon Autodoor Limited		
	115	WO 2005/018137	02/24/05	Securicom Pty Ltd		
	116	WO 2005/029315	03/31/05	Globespanvirata Incorporated		
	117	WO 2005/038729	04/28/05	SCM Microsystems, Inc.		
	118	WO 2006/015625	08/09/04	Telecom Italia S.P.A.		

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	5	of	8	Attorney Docket Number	2943-178

	119	WO 2006/032941	03/30/06	Nokia Corporation		
	120	WO 2006/036521	04/06/06	Qualcomm Incorporated		
	121	WO 2006/126668	11/03/06	NEC Corporation		(Translated Abstract Attached)
	122	WO 2007/103906	09/13/07	Imagineer Software, Inc.		
	123	WO 2007/117315	10/18/07	Symbol Technologies, Inc.		
	124	WO 2007/120215	10/25/07	Imagineer Software, Inc.		
	125	WO 2008/001918	01/03/08	Yui et al.		
	126	WO 2008/010441	01/24/08	NEC Corporation		(Translated Abstract Attached)
	127	EP 1043687	11/22/06	CANON KK		
	128	EP 1148644	10/24/01	COMM RES LAB MINISTRY OF PUBLI		
	129	EP 1292882	03/19/03	ANOTO AB		
	130	EP 1398691	03/17/04	TOSHIBA KK		
	131	EP 1420542	05/19/04	ST MICROELECTRONICS SRL		
	132	EP 1460573	09/22/04	Nokia Corporation		
	133	EP 1643643	04/05/06	MICRONAS GMBH		(Translated Abstract Attached)
	134	EP 1696360	08/30/06	SAMSUNG ELECTRONICS CO LTD		
	135	EP 1760985	03/07/07	Davis et al.		

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	6	of	8	Attorney Docket Number	2943-178

	136	EP 0616429	09/21/94	SIEMENS AG		(Translated Abstract Attached)
	137	EP 0843438	05/20/98	THOMSON MULTIMEDIA SA		
	138	EP 0872976	10/21/98	UNITED TECHNOLOGIES AUTOMOTIVE		
	139	EP 0924894	06/23/99	SIEMENS AG		(Translated Abstract Attached)
	140	EP 0949563	10/13/99	LUCENT TECHNOLOGIES INC		
	141	EP 0996928	05/03/00	ASSURE SYSTEMS INC		

OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)		
Examiner Initials*	Cite No.[1]	
	142	Partial European Search Report for European Patent Application No. 06113988 (Atty File No. 2943-114-EP), dated January 10, 2007.
	143	Written Opinion of the International Searching Authority for International (PCT) Patent Application No. PCT/US2009/053430 (Atty File No. 2943-178-PCT) mailed November 24, 2009.
	144	International Search Report for International (PCT) Patent Application No. PCT/US2009/053430 (Atty File No. 2943-178-PCT) mailed November 24, 2009.
	145	Examiner's First Report for Australian Patent Application No. 2006203768, mailed November 20, 2009.
	146	"Access Control Standard for the 26-Bit Wiegand Reader Interface," Security Industry Association, October 17, 1996, 15 pages.
	147	"Condoplex - The World Leader in Developing Security and Communication Solutions," retrieved from http://web.archive.org/web/20040324112641/http:llcondoplexinc.com/, publication date March 24, 2004, 1 page.
	148	"Contactless Technology for Secure Physical Access: Technology and Standards Choices," Smart Card Alliance White Paper, October 2002, 36 pages.

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	7	of	8	Attorney Docket Number	2943-178

	149	"Information Technology: Application Profile for Commercial Biometrical Physical Access Control," Project INCITS 1706-D, 2005, 16 pages.
	150	"Technology Basics: Understanding Wiegand," HID Corporation, 2004, 5 pages.
	151	ANASHIN, V. "Uniformly distributed sequences over p-adic integers," Number Theoretic and Algebraic Methods in Computer Science, Moscow 1993 (A.J. van der Poorten, I.Shparlinski, and H.G. Zimmer eds., 1995), pp. 1-18, available at http://crypto.rsuh.ru/papers/anashin-paper1.pdf.
	152	ANASHIN, V., "Pseudorandom number generation by p-adic ergodic transformations" (Jan. 29, 2004), available at http://arxiv.org/abs/cs.CR/0401030.
	153	ANASHIN, V., "Pseudorandom number generation by p-adic ergodic transformations: An addendum" (Feb. 26, 2004), pp. 1-9, available at http://arxiv.org/abs/cs.CR/0402060.
	154	ANASHIN, V., "Uniformly distributed sequences in computer algebra, or how to constuct program generators of random numbers," J. Math. Sci., 89(4):1355–1390 (1998), available at http://crypto.rsuh.ru/papers/anashin-paper5.pdf.
	155	ANASHIN, V., "Uniformly distributed sequences of p-adic integers," II. Discrete Math. Appl., 12(6):527–590 (2002), available at http://arXiv.org/abs/math.NT/0209407.
	156	ANASHIN, V., "Uniformly distributed sequences of p-adic integers," Mathematical Notes, 55(2):109–133 (1994), available at http://crypto.rsuh.ru/papers/anashin-paper2.pdf.
	157	BRIAN, M., "How Remote Entry Works," Howstuffworks.com, retrieved from http://auto.howstuffworks.com/remote-entry.htm, printed on May 19,2005, copyright 2005, 8 pages.
	158	DAMGARD, I., "On the Randomness of Legendre and Jacobi Sequences," Advances in Cryptology (Proceedings of Crypto '88), Lecture Notes in Computer Science (1990), pp. 163-172.
	159	Data Sheet, "26 Bit Weigand Specifications," Essex Electronics Incorporated, April 1, 1998, 1 page.
	160	Data Sheet, "Micro RWD EM4001 'Mag swipe' Decimal Output Version," IB Technology, May 3, 2005, pp. 1-8.
	161	DAVIS, M., "Reader To Panel Authentication," Cartes 2005, Paris, France, Nov. 1, 2005, 33 pages.
	162	GLASS, B., "DMCA Used In Garage Door Battle," Ziff Davis Media, retrieved from http://www.extremetech.com/print_article2/0,2533 on May 19, 2005 (Jan. 23,2003), 1 page.
	163	KNEBELKAMP et al., "Latest Generation Technology for Immobilizer Systems," Texas Instruments, retrieved from www.ti.com/tiris on May 19, 2005, 11 pages.

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Scott B. Guthery
				Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	8	of	8	Attorney Docket Number	2943-178

	164	LEVIN, L., "One Way Functions and Pseudorandom Generators," Combinatorica, Vol. 7(4) (1987), pp. 357-363.
	165	Press Release, "Radio Frequency Identification (RFID) based immobilizer systems help to curb auto theft and reduce insurance costs," Texas Instruments, May 7, 1999, 2 pages.
	166	WEINSTEIN, L., "DMCA: Ma Bell Would Be Proud," Wired News, Jan. 20, 2003, 27 pages.
	167	WOODCOCK, F., et al., "p-Adic Chaos and Random Number Generation," Experimental Mathematics, Vol. 7(4), (1998), pp. 334–342.

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference is considered, whether or not citation is in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	secure adj wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 14:42
L3	845	(switch$3 or transition$3) with mode with (ack or acknowledge)	US-PGPUB; USPAT	OR	ON	2012/04/10 14:56
L4	0	(switch$3 or transition$3) with mode with (ack or acknowledge) and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 14:56
L5	903	(switch$3 or transition$3) with mode and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 14:56
L6	11	(switch$3 or transition$3) with mode with packet and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 14:57
L7	9859	(switch$3 or transition$3) with mode with packet	US-PGPUB; USPAT	OR	ON	2012/04/10 14:58
L9	28514	alter$5 with control with signal	US-PGPUB; USPAT	OR	ON	2012/04/10 15:34
L10	101	(switch$3 or transition$3) with wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 15:35
L11	13393	alter$5 with control near1 signal	US-PGPUB; USPAT	OR	ON	2012/04/10 16:05
L13	1406	alter$5 with control near1 signal with time	US-PGPUB; USPAT	OR	ON	2012/04/10 16:05
L14	1300	alter$5 with control adj signal with time	US-PGPUB; USPAT	OR	ON	2012/04/10 16:06
L15	0	alter$5 with control adj signal with time and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 16:06
L16	22	alter$5 with control adj signal and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 16:06
L17	22	alter$5 with control adj2 signal and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 16:07
L18	22	(switch$3 or transition$3) with wiegand and (encrypt$3 or obfuscat$3)	US-PGPUB; USPAT	OR	ON	2012/04/10 16:11
L19	1	(switch$3 or transition$3) with wiegand with packet	US-PGPUB;	OR	ON	2012/04/10 16:35

WAVELYNX EX. 1003, Pg. 1506
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

			USPAT			
L20	5	wiegand with packet	US-PGPUB; USPAT	OR	ON	2012/04/10 16:36
S1	1	"20100034375".pn.	US-PGPUB; USPAT	OR	ON	2012/01/17 09:57
S2	1	("20100235622").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/04/09 15:38
S3	1070	380/46.ccls.	US-PGPUB; USPAT	OR	ON	2012/04/09 15:41
S4	272	380/260.ccls.	US-PGPUB; USPAT	OR	ON	2012/04/09 15:46
S5	114	("20040162863" | "20050182946" | "20060123466" | "20070214293" | "20070294528" | "20070294531" | "20070294539" | "20080061941" | "5357528" | "5446683" | "6285761" | "6810123" | "6944768" | "7212632" | "6724296" | "20030204541" | "20050044119" | "20070043954" | "20070178886" | "5193115" | "5577124" | "6487176" | "7120696" | "6078888" | "20010056534" | "20020184539" | "20030208697" | "20050010624" | "20050110210" | "20060083228" | "20070016942" | "20070076864" | "20070183593" | "20080184349" | "6097307" | "6314440" | "7170997" | "7277543" | "7412056" | "20060177056" | "20070034691" | "20070121943" | "20070165847" | "20070195952" | "20080010218" | "5751808" | "5754603" | "5802176" | "6044388" | "6542608" | "6718038" | "6885747" | "7492905" | "6411199" | "20050265546" | "20060206554" | "20080012690" | "20080046493" | "3694757" | "4087626" | "5533128" | "5608801" | "5680131" | "5686904" | "6079018" | "6154544" | "6606386" | "6608901" | "7118033" | "20010041593" | "20050002533" | "20050129247" | "20060294312" | "20070046424" | "20070057057" | "20070296817" | "20080005532" | "5258936" | "5420928" | "6052786" | "6931533" | "6947560" | "6988203" | "7016925" | "7190787" | "7293698" | "7492898" | "5844990" | "20020016913" | "20040153291" | "20050166040" | "20060174184" | "20070099597" | "20070165848" | "5825882" | "6691141" | "7064665" | "6181252" | "6249866" | "20070109101" | "5696909" | "20030014646" | "20030074319" | "20040162864" | "20060179094" | "20070269048" | "20070293192" | "20080001778" | "20080016363" | "5187676" | "5541996" | "7085791" | "7219113" | "5600324").PN.	US-PGPUB; USPAT	OR	ON	2012/04/09 15:56
S6	15	S5 and rolling with code	US-	OR	ON	2012/04/09

WAVELYNX EX. 1003, Pg. 1507
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

			PGPUB; USPAT			15:57
S7	2	S5 and rolling with code and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/09 15:57
S8	292	(encrypt$3 or obfuscat$3) with rolling adj code	US-PGPUB; USPAT	OR	ON	2012/04/09 17:29
S9	23	(encrypt$3 or obfuscat$3) with rolling adj code and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/09 17:29
S10	273	380/260.ccls.	US-PGPUB; USPAT	OR	ON	2012/04/10 07:59
S11	0	S10 and wiegand and rolling with code	US-PGPUB; USPAT	OR	ON	2012/04/10 07:59
S12	2	S10 and rolling with code	US-PGPUB; USPAT	OR	ON	2012/04/10 07:59
S13	0	S10 and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 08:01
S14	115	(encrypt$3 or obfuscat$3) near2 rolling adj code	US-PGPUB; USPAT	OR	ON	2012/04/10 08:05
S15	1	"20090128392"	US-PGPUB; USPAT	OR	ON	2012/04/10 08:14
S16	1145	roll$3 near key	US-PGPUB; USPAT	OR	ON	2012/04/10 08:18
S17	70	roll$3 near key with encrypt$3	US-PGPUB; USPAT	OR	ON	2012/04/10 08:19
S18	0	roll$3 near key and S10	US-PGPUB; USPAT	OR	ON	2012/04/10 08:20
S19	1	"20070152798"	US-PGPUB; USPAT	OR	ON	2012/04/10 08:35
S20	4	(("5,686,904,") or ("6,175,312,") or ("6,191,707,") or ("6,166,650")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/04/10 08:52
S21	16	rolling with "xor"	US-PGPUB; USPAT	OR	ON	2012/04/10 09:05
S22	114	("20040162863" | "20050182946" | "20060123466" | "20070214293" | "20070294528" | "20070294531" | "20070294539" | "20080061941" | "5357528" | "5446683" | "6285761" | "6810123" | "6944768" | "7212632" | "6724296" | "20030204541" | "20050044119" | "20070043954" | "20070178886" | "5193115" | "5577124" | "6487176" | "7120696" | "6078888" | "20010056534" | "20020184539"	US-PGPUB; USPAT	OR	ON	2012/04/10 10:59

WAVELYNX EX. 1003, Pg. 1508
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

		| "20030208697" | "20050010624" | "20050110210" | "20060083228" | "20070016942" | "20070076864" | "20070183593" | "20080184349" | "6097307" | "6314440" | "7170997" | "7277543" | "7412056" | "20060177056" | "20070034691" | "20070121943" | "20070165847" | "20070195952" | "20080010218" | "5751808" | "5754603" | "5802176" | "6044388" | "6542608" | "6718038" | "6885747" | "7492905" | "6411199" | "20050265546" | "20060206554" | "20080012690" | "20080046493" | "3694757" | "4087626" | "5533128" | "5608801" | "5680131" | "5686904" | "6079018" | "6154544" | "6606386" | "6608901" | "7118033" | "20010041593" | "20050002533" | "20050129247" | "20060294312" | "20070046424" | "20070057057" | "20070296817" | "20080005532" | "5258936" | "5420928" | "6052786" | "6931533" | "6947560" | "6988203" | "7016925" | "7190787" | "7293698" | "7492898" | "5844990" | "20020016913" | "20040153291" | "20050166040" | "20060174184" | "20070099597" | "20070165848" | "5825882" | "6691141" | "7064665" | "6181252" | "6249866" | "20070109101" | "5696909" | "20030014646" | "20030074319" | "20040162864" | "20060179094" | "20070269048" | "20070293192" | "20080001778" | "20080016363" | "5187676" | "5541996" | "7085791" | "7219113" | "5600324").PN.				
S23	11	S22 and (collid$3 or collision)	US-PGPUB; USPAT	OR	ON	2012/04/10 10:59
S24	147	"xor" with stream adj cipher	US-PGPUB; USPAT	OR	ON	2012/04/10 11:21
S25	15	"xor" with stream adj cipher and infrared	US-PGPUB; USPAT	OR	ON	2012/04/10 11:21
S26	7	(ack or acknowledgement) with out adj band and (unidirectional or uni adj directional or one adj way)	US-PGPUB; USPAT	OR	ON	2012/04/10 12:03
S27	15	(ack or acknowledgement) with out adj band and (infrared or IR or RF or radio adj frequency)	US-PGPUB; USPAT	OR	ON	2012/04/10 12:04

EAST Search History (Interference)

<This search history is empty>

4/ 10/ 2012 5:10:35 PM
C:\ Users\ czecher\ Documents\ EAST\ Workspaces\ 12539431.wsp

WAVELYNX EX. 1003, Pg. 1509
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9292

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
12/539,431	08/11/2009	380	2432	2943AAAB-178

APPLICANTS

Michael Davis, Amherst, NY;
David Andresky, Lafayette, CO;
Scott B. Guthery, Chestnut Hill, MA;
Mark Robinton, Somerville, MA;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/087,941 08/11/2008

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

08/20/2009

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /CORDELIA P K ZECHER/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		NY	5	40	4

ADDRESS

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202
UNITED STATES

TITLE

SECURE WIEGAND COMMUNICATIONS

FILING FEE RECEIVED		
2480	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

WAVELYNX EX. 1003, Pg. 1510
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	1

Complete if Known	
Application Number	12/539,431
Filing Date	August 11, 2009
First Named Inventor	Michael Davis
Art Unit	2432
Examiner Name	Cordelia P.K. Zecher
Attorney Docket Number	2943-178

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	1	EP 0697491	2/21/1996	NIPPON DENSO CO		
	2	WO 02/082367	10/17/2002	PITTWAY CORP		
	3	WO 2008/043125	4/17/2008	MICROLATCH PTY LTD		

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Sheet	1	of	1	Attorney Docket Number	2943-178

Complete if Known	
Application Number	12/539,431
Filing Date	August 11, 2009
First Named Inventor	Michael Davis
Art Unit	2432
Examiner Name	Cordelia P.K. Zecher

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	4	European Search Report and Opinion for European Patent Application No. EP09807178, dated Nov. 08, 2011 (Attorney's Ref. No. 2943-178-PEP) 6 pages
	5	Official Action for U.S. Patent Application No. 11/464,912, mailed Jun. 2, 2010 (Attorney Ref. No. 2943-114)
	6	Official Action for U.S. Patent Application No. 11/464,912, mailed Nov. 23, 2010 (Attorney Ref. No. 2943-114)
	7	Notice of Allowance for U.S. Patent Application No. 11/464,912, mailed Jan. 20, 2012 (Attorney's Ref. No. 2943-114) 5 pages

Examiner Signature	/Cordelia Zecher/	Date Considered	04/09/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.
This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO:**
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2432
	)	
GUTHERY et al.	)	Examiner: ZECHER, CORDELIA P K
	)	
Serial No.: 12/539,431	)	Confirmation No.: 9292
	)	
Filed: August 11, 2009	)	
	)	
Atty. File No.: 2943AAAB-178	)	
	)	
For:'SECURE WIEGAND COMMUNICATIONS'	)	
	)	

AMENDMENT AND RESPONSE

Mailstop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

Applicant submits this Amendment and Response to address the Office Action having a mailing date of April 13, 2012. Submitted herewith is a Petition for a one-month Extension of Time, together with the required fee. Although Applicant believes that no additional fees are due in connection with filing this Amendment and Response, please charge any additional fees deemed necessary, or credit any overpayment, to Deposit Account No. 19-1970.

Please amend the above-identified patent application as follows:

Amendments to the Claims are shown in the listing of claims which begins on page **2** of this paper.

Remarks begin on page **7** of this paper.

WAVELYNX EX. 1003, Pg. 1513
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A communication method, comprising:

obfuscating data transmitted in a first message from a first communication device to a second communication device, wherein the first and second communication devices communicate using a unidirectional communication protocol and wherein the obfuscation of the data is effected with a predetermined code wherein the first communication device is upstream of the second communication device, the method further comprising:

determining that the message received at the first communication device was transmitted by the second communication device, wherein determining is performed by one or more of (i) analyzing an out-of-band communication received at the first communication device from the second communication device and (ii) analyzing a special code that identifies the second communication device is an advanced communication device in an advanced communication mode; and

based on determining that the message was transmitted by the second communication device, transitioning the first communication device from a first mode of operation to a second mode of operation, wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode.

2. (Original) The method of claim 1, wherein the predetermined code is agreed upon between the first and second communication devices prior to obfuscation of the data in the first message.

3. (Original) The method of claim 1, wherein the predetermined code is one of a plurality of codes within a rolling code sequence, wherein the first and second communication devices each have a copy of the rolling code sequence and wherein data communicated between the first and second communication devices subsequent to the

WAVELYNX EX. 1003, Pg. 1514
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

first message is obfuscated with a code from the rolling code sequence that is different from the predetermined code.

4. (Original) The method of claim 1, wherein the unidirectional communication protocol comprises the Wiegand protocol.

5. (Original) The method of claim 4, wherein the first message comprises a Wiegand message.

6. (Original) The method of claim 5, wherein the Wiegand message is encapsulated in one of a TCP and UDP packet and is transmitted over an IP network from the first communication device to the second communication device.

7. (Original) The method of claim 1, wherein obfuscation comprises computing an XOR of the predetermined code and the data.

8. (Original) The method of claim 1, wherein the predetermined code is employed to identify an authenticity of the first communication device and a timestamp.

9. (Canceled)

10. (Currently Amended) The method of ~~claim 9~~claim 1, wherein the message transmitted by the second communication device comprises an alteration of a control line signal between the first and second communication devices for a predetermined amount of time.

11. (Currently Amended) The method of claim 10, wherein the predetermined amount of time is less than ~~a human-perceivable amount of time~~10ms.

WAVELYNX EX. 1003, Pg. 1515
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

12. (Currently Amended) The method of ~~claim 9~~claim 1, wherein ~~the first mode comprises a non-secure Wiegand mode and the second mode comprises a secure Wiegand mode~~the message was transmitted over a Wiegand wire.

13. (Currently Amended) The method of claim ~~9, wherein the first mode comprises a Wiegand format mode and the second mode comprises a packet mode~~12, wherein the message was transmitted over an LEDCTL line of the Wiegand wire.

14. (Original) The method of claim 1, further comprising:

detecting a message collision on a communication path between the first and second communication devices; and

initiating a cooperative transmission of messages over the communication path such that the first communication device transmits a message to the second communication device over the communication path at a different time than the second communication device transmits a message to the first communication device over the communication path.

15. (Original) The method of claim 1, wherein out-of-band communications are transmitted from the second communication device to the first communication device at a timing different from message timing used in the unidirectional protocol.

16. (Original) The method of claim 1, wherein control signals are used to accommodate bi-directional communications in one of a half-duplex configuration and a full-duplex configuration.

17. (Original) The method of claim 1, wherein the obfuscation is accomplished by the use of a stream cipher.

18. (Original) The method of claim 1, wherein the first message maintains the same size before and after being obfuscated.

WAVELYNX EX. 1003, Pg. 1516
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

19. (Currently Amended) A reader, comprising:

a rolling code generator operable to generate a plurality of distinct rolling codes; and

a message formatting engine, wherein the message formatting engine is operable to retrieve a first rolling code from the rolling code generator and obfuscate data with the first rolling code prior to transmitting the data to an upstream device, wherein the reader is further operable to receive a message from the upstream device, determine that the received message received was transmitted by the upstream device, and based on determining that the message was transmitted by the upstream device, transition from operating in a first mode of operation to a second mode of operation, wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode.

20. (Original) The reader of claim 19, wherein the upstream device also has a copy of the rolling codes, wherein data communicated to the upstream device after using the first rolling code is obfuscated with a code from the rolling code sequence that is different from the first rolling code.

21. (Original) The reader of claim 19, wherein a unidirectional communication protocol is used to facilitate communications between the reader and the upstream device, and wherein the unidirectional communication protocol comprises the Wiegand protocol.

22. (Original) The reader of claim 19, wherein obfuscation comprises computing an XOR of the first rolling code and the data.

23. (Original) The reader of claim 19, wherein the first rolling code is used to confirm an identity of the reader to the upstream device.

24. (Canceled)

WAVELYNX EX. 1003, Pg. 1517
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

25. (Currently Amended) The reader of ~~claim 24~~claim 19, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time.

26. (Currently Amended) The reader of claim 25, wherein the predetermined amount of time is less than ~~a human-perceivable amount of time~~10ms.

27. (Currently Amended) The reader of claim 24, wherein ~~the first mode comprises a non-secure Wiegand mode and the second mode comprises a secure Wiegand mode~~the message is transmitted over a Wiegand wire.

28. (Currently Amended) The reader of ~~claim 24~~claim 27, ~~wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode~~the message is transmitted over an LEDCTL line of the Wiegand wire.

29. (Original) The reader of claim 19, wherein the reader is further operable to detect a message collision on a shared communication path between the reader and upstream device and initiate a cooperative transmission of messages over the shared communication path with the upstream device.

30-40. (Canceled)

WAVELYNX EX. 1003, Pg. 1518
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

REMARKS

The above-identified patent application has been reviewed in light of the Examiner's Action dated April 13, 2012. Claims 1, 10, 11, 12, 13, 19, 25, 26, 27, and 28 have been amended and claims 9, 24, and 30-40 have been canceled without intending to abandon or to dedicate to the public any patentable subject matter. Accordingly, claims 1-8, 10-23, and 25-29 are now pending.

Rejections Under 35 U.S.C. §112

Claim 11 has been rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. Claim 11 has been amended to replace "a human perceivable amount of time" with "10ms" per the originally-filed application at, for example, page 30, lines 15-18. Accordingly, it is respectfully requested that the rejection of claim 11 be reconsidered and withdrawn.

Rejections Under 35 U.S.C. §§102 and 103

Claims 1-3, 7, 16, 19, 20, and 22 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication No. 2009/0128392 to Hardacker et al. ("Hardacker").

In order for a rejection under 35 U.S.C. § 102 to be proper, each and every claim element must be found in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987).

Claims 4-6, 8-15, 17, 18, 21, and 23-29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over various combination of Hardacker, U.S. Patent Publication No. 2007/0046424 to Davis ("Davis '424"), U.S. Patent Publication No. 2006/0123466 to Davis et al. ("Davis '466"), U.S. Patent Publication No. 2008/0037466 to Ngo et al. ("Ngo"), and U.S. Patent Publication No. 2006/0210081 to Zhu et al. ("Zhu").

When determining whether a claim is obvious under 35 U.S.C. § 103, an examiner must make "a searching comparison of the claimed invention–***including all its limitations***–with the teaching of the prior art." *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis added). Thus, "obviousness requires a suggestion of all limitations in a

WAVELYNX EX. 1003, Pg. 1519
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

claim." *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003) (citing *In re Royka*, 490 F.2d 981, 985 (CCPA 1974) (holding that to establish prima facie obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art)). Applicant respectfully submits that several features in the pending claims are neither taught nor suggested, either expressly or inherently, in any of the cited prior art references. Accordingly, for at least the reasons below, Applicant submits that the rejections of the claims under 35 U.S.C. 103 should be reconsidered and withdrawn.

More specifically, independent claim 1 has been amended to recite, *inter alia*, based on determining that the message was transmitted by the second communication device, transitioning the first communication device from a first mode of operation to a second mode of operation, wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode. Claim 19 has been amended to recite, *inter alia,* wherein the reader is further operable to receive a message from the upstream device, determine that the received message received was transmitted by the upstream device, and based on determining that the message was transmitted by the upstream device, transition from operating in a first mode of operation to a second mode of operation, wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode. The Examiner has correctly indicated that Hardacker fails to teach such a feature. *See Office Action* at page 6, item 15. The Examiner argues, however, that such a feature is found in Davis '466. Applicant respectfully disagrees.

Davis '466 only discloses the concept of a "Wiegand Extension" where extension bits are transmitted between a reader and panel. Contrary to the Examiner's assertion, there is absolutely no disclosure in Davis '466 of causing a reader to transition from a first mode of operation to a second mode of operation where the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode. Indeed, there is absolutely no disclosure in Davis '466 of having a Wiegand reader operated in a packet-mode. The advantages of having a reader configured to transition into a packet-mode of operation are described in detail in the originally-filed application at, for example, pages 29-33 and pages 38-40.

WAVELYNX EX. 1003, Pg. 1520
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

To the extent that the prior art fails to teach all aspects of the currently-pending independent claims, Applicant submits that the rejection of claims 1 and 19 and the dependent claims therefrom should be reconsidered and withdrawn.

In addition to being dependent from an allowable independent claim, the dependent claims provide further reasons for allowance. For instance, dependent claim 10, 11, 25, and 26 recite that a message transmitted by the second communication device to cause the first communication device to transition to the packet-mode of operation comprises an alteration of a control signal between the devices for a predetermined amount of time, namely less than 10ms. This specific message configuration is not disclosed in any of the prior art references. The Examiner has generally referred to the table between paragraphs [0032] and [0033] of Davis '466, but this table only discloses bit values for commands sent by the panel. There is absolutely no disclosure of a message as claimed in claims 10, 11, 25, and 26.

As another example, dependent claim 12, 13, 27, and 28 recite details related to the wire over which the transition-inducing message is transmitted. There is no disclosure of causing a reader to transition to a packet-mode of operation, let alone causing a reader to perform such a function by transmitting messages of a Wiegand wire, namely the LEDCTL line of the Wiegand wire.

Based upon the foregoing, Applicant believes that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: August 13, 2012

By: /Matthew R. Ellsworth/
Matthew R. Ellsworth
Reg. No. 56,345
Telephone: 303-863-2989

WAVELYNX EX. 1003, Pg. 1521
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

PTO/SB/22 (09-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARMENT OF COMMERCE
Under the paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 2943AAAB-178
Application Number 12/539,431	Filed 2009-08-11
For SECURE WIEGAND COMMUNICATIONS	
Art Unit 2432	Examiner ZECHER, CORDELIA P K

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	
☑	One month (37 CFR 1.17(a)(1))	$150	$75	$ 150
☐	Two months (37 CFR 1.17(a)(2))	$560	$280	$
☐	Three months (37 CFR 1.17(a)(3))	$1270	$635	$
☐	Four months (37 CFR 1.17(a)(4))	$1980	$990	$
☐	Five months (37 CFR 1.17(a)(5))	$2690	$1345	$

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 191970.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration Number 56,345

☐ attorney or agent under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Matthew R. Ellsworth/ — Signature

2012-08-13 — Date

Matthew R. Ellsworth — Typed or printed name

(303) 863-9700 — Telephone Number

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☐ Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	12539431
Filing Date:	11-Aug-2009
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Attorney Docket Number:	2943AAAB-178

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	150	150

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**150**

Electronic Acknowledgement Receipt	
EFS ID:	13486199
Application Number:	12539431
International Application Number:	
Confirmation Number:	9292
Title of Invention:	SECURE WIEGAND COMMUNICATIONS
First Named Inventor/Applicant Name:	Michael Davis
Customer Number:	22442
Filer:	Matthew Ryan Ellsworth/Leslie Roberts
Filer Authorized By:	Matthew Ryan Ellsworth
Attorney Docket Number:	2943AAAB-178
Receipt Date:	13-AUG-2012
Filing Date:	11-AUG-2009
Time Stamp:	18:32:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$150
RAM confirmation Number	6489
Deposit Account	191970
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees) Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees) Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	**Document Description**	**File Name**	**File Size(Bytes)/ Message Digest**	**Multi Part /.zip**	**Pages (if appl.)**
1		AMEND_01.pdf	132807 002fd459df808ff51b6b4db51e71570deff01aa7	yes	9
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	6	
	Applicant Arguments/Remarks Made in an Amendment		7	9	
Warnings:					
Information:					
2	Extension of Time	EXTENSION_OF_TIME.pdf	286299 880d9a1a2d3a41f84dae3924b4d77c2ddd3a504a	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30469 d0fab17a6358be63015f892c9da77f455fd2b84c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	449575		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
12/539,431	08/11/2009	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 08/13/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 27	Minus	** 40	= 0	X $ =		OR	X $60=	0
Independent (37 CFR 1.16(h))	* 2	Minus	***4	= 0	X $ =		OR	X $250=	0
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/NICOLLE L. SCRIVNER/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

22442 7590 08/31/2012

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER	
ZECHER, CORDELIA P K	
ART UNIT	PAPER NUMBER
2432	

DATE MAILED: 08/31/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/539,431	08/11/2009	Michael Davis	2943AAAB-178	9292

TITLE OF INVENTION: SECURE WIEGAND COMMUNICATIONS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1740	$300	$0	$2040	11/30/2012

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 02/11)

WAVELYNX EX. 1003, Pg. 1530
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22442 7590 08/31/2012

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/539,431	08/11/2009	Michael Davis	2943AAAB-178	9292

TITLE OF INVENTION: SECURE WIEGAND COMMUNICATIONS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1740	$300	$0	$2040	11/30/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
ZECHER, CORDELIA P K	2432	380-262000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

WAVELYNX EX. 1003, Pg. 1531
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/539,431	08/11/2009	Michael Davis	2943AAAB-178	9292

22442 7590 08/31/2012

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER	
ZECHER, CORDELIA P K	
ART UNIT	PAPER NUMBER
2432	

DATE MAILED: 08/31/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 441 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 441 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

WAVELYNX EX. 1003, Pg. 1532
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	12/539,431	DAVIS ET AL.	
	Examiner	Art Unit	
	CORDELIA ZECHER	2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *CORDELIA ZECHER*. (3)_____.

(2) *Matthew Ellsworth*. (4)_____.

Date of Interview: *27 August 2012*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *24 and 27*.

Identification of prior art discussed: _____.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Claim 27 depended from claim 24, however claim 24 was cancelled. Applicant's representative approved an amendment to change claim 27 to depend from independent claim 19.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/CORDELIA ZECHER/ Examiner, Art Unit 2432	

WAVELYNX EX. 1003, Pg. 1534
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Notice of Allowability	Application No.	Applicant(s)	
	12/539,431	DAVIS ET AL.	
	Examiner	Art Unit	
	CORDELIA ZECHER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Interview 8/27/12*.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-8,10-23 and 25-29*.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/CORDELIA ZECHER/
Examiner, Art Unit 2432

WAVELYNX EX. 1003, Pg. 1535
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Matthew Ellsworth on August 27, 2012.

The application has been amended as follows:

Claim 27 (currently amended) The reader of claim ~~24~~ 19, wherein the message is transmitted over a Wiegand wire.

EXAMINER'S COMMENTS

This communication warrants No Examiner's Reason for Allowance, applicant's reply make evident the reasons for allowance, satisfying the "record as a whole" proviso of the rule 37 CFR 1.104(e). Specifically, applicant's arguments filed on August 13, 2012 are persuasive, as such the reasons for allowance are in all probability evident from the record and no statement is deemed necessary (see MPEP 1302.14).

Any comments Applicants considers necessary must be submitted no later than the payment of the Issue Fee and to avoid processing delays, should preferable accompany the Issue Fees. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance". In event of any post-allowance papers (e.g. IDS, 312 amendment, petition, etc.), Applicant is exhorted to mail papers to the Production Control branch in Publications or faxed to post-allowance papers correspondence

branch at (703) 308-5864 to expedite issuing process or call PUB's Customer Service if any questions at (703) 305-8497.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA ZECHER whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CORDELIA ZECHER/
Examiner, Art Unit 2432

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12539431	DAVIS ET AL.
	Examiner	Art Unit
	CORDELIA ZECHER	2432

SEARCHED			
Class	Subclass	Date	Examiner
380	260	8/27/12	cz
380	270	8/27/12	cz

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Search	4/9/12	cz
Searched EAST (see attached)	8/27/12	cz

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
380	270 (see attached)	8/27/12	cz

WAVELYNX EX. 1003, Pg. 1538
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9292

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
12/539,431	08/11/2009	380	2432	2943AAAB-178

APPLICANTS

Michael Davis, Amherst, NY;
David Andresky, Lafayette, CO;
Scott B. Guthery, Chestnut Hill, MA;
Mark Robinton, Somerville, MA;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/087,941 08/11/2008

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

08/20/2009

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /CORDELIA P K ZECHER/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		NY	5	40	4

ADDRESS

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202
UNITED STATES

TITLE

SECURE WIEGAND COMMUNICATIONS

FILING FEE RECEIVED		
2480	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

WAVELYNX EX. 1003, Pg. 1539
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12539431	DAVIS ET AL.
	Examiner	**Art Unit**
	CORDELIA ZECHER	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/09/2012	08/27/2012							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
4	4	✓	=							
5	5	✓	=							
6	6	✓	=							
7	7	✓	=							
8	8	✓	=							
	9	✓	-							
9	10	✓	=							
10	11	✓	=							
11	12	✓	=							
12	13	✓	=							
13	14	✓	=							
14	15	✓	=							
15	16	✓	=							
16	17	✓	=							
17	18	✓	=							
18	19	✓	=							
19	20	✓	=							
20	21	✓	=							
21	22	✓	=							
22	23	✓	=							
	24	✓	-							
23	25	✓	=							
24	26	✓	=							
25	27	✓	=							
26	28	✓	=							
27	29	✓	=							
	30	N	-							
	31	N	-							
	32	N	-							
	33	N	-							
	34	N	-							
	35	N	-							
	36	N	-							

WAVELYNX EX. 1003, Pg. 1540
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12539431	DAVIS ET AL.
	Examiner	**Art Unit**
	CORDELIA ZECHER	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/09/2012	08/27/2012							
	37	N	-							
	38	N	-							
	39	N	-							
	40	N	-							

WAVELYNX EX. 1003, Pg. 1541
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L5	1	"6988203".pn.	US-PGPUB; USPAT	OR	ON	2012/08/27 11:11
L6	6	wiegand with packet	US-PGPUB; USPAT	OR	ON	2012/08/27 11:17
L7	1	wiegand with udp	US-PGPUB; USPAT	OR	ON	2012/08/27 11:24
L8	32	wiegand with (tcp or tranmission adj control adj protocol or http or hypertext adj transfer adj protocol or snmp or simple adj network adj management adj protocol)	US-PGPUB; USPAT	OR	ON	2012/08/27 11:26
L9	133	davis-michael.in.	US-PGPUB; USPAT	OR	ON	2012/08/27 11:34
L10	5	9 and wiegand	US-PGPUB; USPAT	OR	ON	2012/08/27 11:34
L11	283	380/260.ccls.	US-PGPUB; USPAT	OR	ON	2012/08/27 11:45
L12	1967	380/270.ccls.	US-PGPUB; USPAT	OR	ON	2012/08/27 11:46
L13	1102	380/46.ccls.	US-PGPUB; USPAT	OR	ON	2012/08/27 11:46
L14	1	(wiegand and (packet or tcp or udp or http or snmp) and (transition$3 or switch$3) and rolling adj code).clm.	US-PGPUB; USPAT	OR	ON	2012/08/27 11:48
S1	1	"20100034375".pn.	US-PGPUB; USPAT	OR	ON	2012/01/17 09:57
S2	1	("20100235622").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/04/09 15:38
S3	1070	380/46.ccls.	US-PGPUB; USPAT	OR	ON	2012/04/09 15:41
S4	272	380/260.ccls.	US-PGPUB; USPAT	OR	ON	2012/04/09 15:46
S5	114	("20040162863" | "20050182946" | "20060123466" | "20070214293" | "20070294528" | "20070294531" | "20070294539" | "20080061941" | "5357528"	US-PGPUB; USPAT	OR	ON	2012/04/09 15:56

WAVELYNX EX. 1003, Pg. 1542
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

		| "5446683" | "6285761" | "6810123" | "6944768" | "7212632" | "6724296" | "20030204541" | "20050044119" | "20070043954" | "20070178886" | "5193115" | "5577124" | "6487176" | "7120696" | "6078888" | "20010056534" | "20020184539" | "20030208697" | "20050010624" | "20050110210" | "20060083228" | "20070016942" | "20070076864" | "20070183593" | "20080184349" | "6097307" | "6314440" | "7170997" | "7277543" | "7412056" | "20060177056" | "20070034691" | "20070121943" | "20070165847" | "20070195952" | "20080010218" | "5751808" | "5754603" | "5802176" | "6044388" | "6542608" | "6718038" | "6885747" | "7492905" | "6411199" | "20050265546" | "20060206554" | "20080012690" | "20080046493" | "3694757" | "4087626" | "5533128" | "5608801" | "5680131" | "5686904" | "6079018" | "6154544" | "6606386" | "6608901" | "7118033" | "20010041593" | "20050002533" | "20050129247" | "20060294312" | "20070046424" | "20070057057" | "20070296817" | "20080005532" | "5258936" | "5420928" | "6052786" | "6931533" | "6947560" | "6988203" | "7016925" | "7190787" | "7293698" | "7492898" | "5844990" | "20020016913" | "20040153291" | "20050166040" | "20060174184" | "20070099597" | "20070165848" | "5825882" | "6691141" | "7064665" | "6181252" | "6249866" | "20070109101" | "5696909" | "20030014646" | "20030074319" | "20040162864" | "20060179094" | "20070269048" | "20070293192" | "20080001778" | "20080016363" | "5187676" | "5541996" | "7085791" | "7219113" | "5600324").PN.				
S6	15	S5 and rolling with code	US-PGPUB; USPAT	OR	ON	2012/04/09 15:57
S7	2	S5 and rolling with code and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/09 15:57
S8	292	(encrypt$3 or obfuscat$3) with rolling adj code	US-PGPUB; USPAT	OR	ON	2012/04/09 17:29
S9	23	(encrypt$3 or obfuscat$3) with rolling adj code and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/09 17:29
S10	273	380/260.ccls.	US-PGPUB; USPAT	OR	ON	2012/04/10 07:59
S11	0	S10 and wiegand and rolling with code	US-PGPUB; USPAT	OR	ON	2012/04/10 07:59
S12	2	S10 and rolling with code	US-PGPUB; USPAT	OR	ON	2012/04/10 07:59

WAVELYNX EX. 1003, Pg. 1543
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

S13	0	S10 and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 08:01
S14	115	(encrypt$3 or obfuscat$3) near2 rolling adj code	US-PGPUB; USPAT	OR	ON	2012/04/10 08:05
S15	1	"20090128392"	US-PGPUB; USPAT	OR	ON	2012/04/10 08:14
S16	1145	roll$3 near key	US-PGPUB; USPAT	OR	ON	2012/04/10 08:18
S17	70	roll$3 near key with encrypt$3	US-PGPUB; USPAT	OR	ON	2012/04/10 08:19
S18	0	roll$3 near key and S10	US-PGPUB; USPAT	OR	ON	2012/04/10 08:20
S19	1	"20070152798"	US-PGPUB; USPAT	OR	ON	2012/04/10 08:35
S20	4	(("5,686,904,") or ("6,175,312,") or ("6,191,707,") or ("6,166,650")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/04/10 08:52
S21	16	rolling with "xor"	US-PGPUB; USPAT	OR	ON	2012/04/10 09:05
S22	114	("20040162863" | "20050182946" | "20060123466" | "20070214293" | "20070294528" | "20070294531" | "20070294539" | "20080061941" | "5357528" | "5446683" | "6285761" | "6810123" | "6944768" | "7212632" | "6724296" | "20030204541" | "20050044119" | "20070043954" | "20070178886" | "5193115" | "5577124" | "6487176" | "7120696" | "6078888" | "20010056534" | "20020184539" | "20030208697" | "20050010624" | "20050110210" | "20060083228" | "20070016942" | "20070076864" | "20070183593" | "20080184349" | "6097307" | "6314440" | "7170997" | "7277543" | "7412056" | "20060177056" | "20070034691" | "20070121943" | "20070165847" | "20070195952" | "20080010218" | "5751808" | "5754603" | "5802176" | "6044388" | "6542608" | "6718038" | "6885747" | "7492905" | "6411199" | "20050265546" | "20060206554" | "20080012690" | "20080046493" | "3694757" | "4087626" | "5533128" | "5608801" | "5680131" | "5686904" | "6079018" | "6154544" | "6606386" | "6608901" | "7118033" | "20010041593" | "20050002533" | "20050129247" | "20060294312" | "20070046424" | "20070057057" | "20070296817" | "20080005532" | "5258936" | "5420928" | "6052786" | "6931533" | "6947560" | "6988203" | "7016925" | "7190787" | "7293698" | "7492898" |	US-PGPUB; USPAT	OR	ON	2012/04/10 10:59

WAVELYNX EX. 1003, Pg. 1544
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

		"5844990" | "20020016913" | "20040153291" | "20050166040" | "20060174184" | "20070099597" | "20070165848" | "5825882" | "6691141" | "7064665" | "6181252" | "6249866" | "20070109101" | "5696909" | "20030014646" | "20030074319" | "20040162864" | "20060179094" | "20070269048" | "20070293192" | "20080001778" | "20080016363" | "5187676" | "5541996" | "7085791" | "7219113" | "5600324").PN.				
S23	11	S22 and (collid$3 or collision)	US-PGPUB; USPAT	OR	ON	2012/04/10 10:59
S24	147	"xor" with stream adj cipher	US-PGPUB; USPAT	OR	ON	2012/04/10 11:21
S25	15	"xor" with stream adj cipher and infrared	US-PGPUB; USPAT	OR	ON	2012/04/10 11:21
S26	7	(ack or acknowledgement) with out adj band and (unidirectional or uni adj directional or one adj way)	US-PGPUB; USPAT	OR	ON	2012/04/10 12:03
S27	15	(ack or acknowledgement) with out adj band and (infrared or IR or RF or radio adj frequency)	US-PGPUB; USPAT	OR	ON	2012/04/10 12:04
S28	2	secure adj wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 14:42
S29	845	(switch$3 or transition$3) with mode with (ack or acknowledge)	US-PGPUB; USPAT	OR	ON	2012/04/10 14:56
S30	0	(switch$3 or transition$3) with mode with (ack or acknowledge) and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 14:56
S31	903	(switch$3 or transition$3) with mode and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 14:56
S32	11	(switch$3 or transition$3) with mode with packet and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 14:57
S33	9859	(switch$3 or transition$3) with mode with packet	US-PGPUB; USPAT	OR	ON	2012/04/10 14:58
S34	28514	alter$5 with control with signal	US-PGPUB; USPAT	OR	ON	2012/04/10 15:34
S35	101	(switch$3 or transition$3) with wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 15:35
S36	13393	alter$5 with control near1 signal	US-PGPUB; USPAT	OR	ON	2012/04/10 16:05
S37	1406	alter$5 with control near1 signal with time	US-PGPUB; USPAT	OR	ON	2012/04/10 16:05
S38	1300	alter$5 with control adj signal with time	US-PGPUB;	OR	ON	2012/04/10 16:06

WAVELYNX EX. 1003, Pg. 1545
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

			USPAT			
S39	0	alter$5 with control adj signal with time and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 16:06
S40	22	alter$5 with control adj signal and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 16:06
S41	22	alter$5 with control adj2 signal and wiegand	US-PGPUB; USPAT	OR	ON	2012/04/10 16:07
S42	22	(switch$3 or transition$3) with wiegand and (encrypt$3 or obfuscat$3)	US-PGPUB; USPAT	OR	ON	2012/04/10 16:11
S43	1	(switch$3 or transition$3) with wiegand with packet	US-PGPUB; USPAT	OR	ON	2012/04/10 16:35
S44	5	wiegand with packet	US-PGPUB; USPAT	OR	ON	2012/04/10 16:36

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L15	0	(wiegand and (packet or tcp or udp or http or snmp) and (transition$3 or switch$3) and rolling adj code).clm.	USPAT	OR	ON	2012/08/27 11:48
L16	262	380/260.ccls.	USPAT	OR	ON	2012/08/27 11:48
L17	979	380/270.ccls.	USPAT	OR	ON	2012/08/27 11:48
L18	0	15 and 17	USPAT	OR	ON	2012/08/27 11:48

8/ 27/ 2012 2:57:01 PM
C:\ Users\ czecher\ Documents\ EAST\ Workspaces\ 12539431.wsp

WAVELYNX EX. 1003, Pg. 1546
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12539431	DAVIS ET AL.
	Examiner	**Art Unit**
	CORDELIA ZECHER	2432

ORIGINAL		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
380	270	H	0	4	K	1 / 00 (2006.01.01)						

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
380	260	46			

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	27	
/CORDELIA ZECHER/ Examiner.Art Unit 2432	08/27/2012	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

WAVELYNX EX. 1003, Pg. 1547
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/539,431	08/11/2009	Michael Davis	2943AAAB-178	9292

22442 7590 10/17/2012

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER	
ZECHER, CORDELIA P K	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
10/17/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

WAVELYNX EX. 1003, Pg. 1548
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Notice of Allowability	Application No.	Applicant(s)	
	12/539,431	DAVIS ET AL.	
	Examiner	Art Unit	
	CORDELIA ZECHER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Interview 10/15/12*.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-8,10-23 and 25-29*.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/CORDELIA ZECHER/
Primary Examiner, Art Unit 2432

WAVELYNX EX. 1003, Pg. 1549
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	12/539,431	DAVIS ET AL.	
	Examiner	Art Unit	
	CORDELIA ZECHER	2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *CORDELIA ZECHER*. (3)_____.

(2) *Matthew Ellsworth*. (4)_____.

Date of Interview: *15 October 2012*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: _____.

Issues Discussed ☒101 ☐112 ☐102 ☐103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *19*.

Identification of prior art discussed: _____.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Amending claim 19 to include one of a microprocessor or firmware was discussed. Applicant's representative agreed to the amendment.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/CORDELIA ZECHER/ Primary Examiner, Art Unit 2432	

WAVELYNX EX. 1003, Pg. 1550
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Matthew Ellsworth on October 15, 2012.

The application has been amended as follows:

19. (Currently Amended) A reader, comprising:

at least one of a microprocessor or firmware;

a rolling code generator operable to generate a plurality of distinct rolling codes; and

a message formatting engine, wherein the message formatting engine is operable to retrieve a first rolling code from the rolling code generator and obfuscate data with the first rolling code prior to transmitting the data to an upstream device, wherein the reader is further operable to receive a message from the upstream device, and based on determining that the message was transmitted by the upstream device, transition from operating in a first mode of operation to a second mode of operation, wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet mode.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA ZECHER whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CORDELIA ZECHER/
Primary Examiner, Art Unit 2432

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
(Use as many sheets as necessary)				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	1	of	5	Attorney Docket Number	2943AAAB-178

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	3842350	10/15/1974	Gross	
	2	4163215	07/31/1979	Iida	
	3	4333072	06/01/1982	Beigel	
	4	4425645	01/10/1984	Weaver et al.	
	5	4519068	05/21/1985	Krebs et al.	
	6	4549264	10/22/1985	Carroll et al.	
	7	4656463	04/07/1987	Anders et al.	
	8	4688026	08/18/1987	Scribner et al.	
	9	4849927	07/18/1989	Vos	
	10	5013898	05/07/1991	Glasspool	
	11	5028918	07/02/1991	Giles et al.	
	12	5041826	08/20/1991	Milheiser	
	13	5050150	09/17/1991	Ikeda	
	14	5151684	09/29/1992	Johnsen	
	15	5166676	11/24/1992	Milheiser	
	16	5218344	06/08/1993	Ricketts	
	17	5235642	08/10/1993	Wobber et al.	
	18	5343469	08/30/1994	Ohshima	
	19	5347263	09/13/1994	Carroll et al.	
	20	5396215	03/07/1995	Hinkle	
	21	5426425	06/20/1995	Comad et al.	
	22	5467082	11/14/1995	Sanderson	
	23	5491471	02/13/1996	Stobbe	
	24	5517172	05/14/1996	Chiu	
	25	5519381	05/21/1996	Marsh et al.	
	26	5521602	05/28/1996	Carroll et al.	
	27	5594384	01/14/1997	Carroll et al.	
	28	5600683	02/04/1997	Bierach et al.	
	29	5679945	10/21/1997	Renner et al.	
	30	5724417	03/03/1998	Bartholomew et al.	
	31	5745037	04/28/1998	Guthrie et al.	
	32	5777561	07/07/1998	Chieu et al.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
(Use as many sheets as necessary)				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	2	of	5	Attorney Docket Number	2943AAAB-178

	33	5848541	12/15/1998	Glick et al.	
	34	5886894	03/23/1999	Rakoff	
	35	5887176	03/23/1999	Griffith et al.	
	36	5909462	06/01/1999	Kamerman et al.	
	37	5923264	07/13/1999	Lavelle et al.	
	38	5929779	07/27/1999	MacLellan et al.	
	39	5952922	09/14/1999	Shober	
	40	5952935	09/14/1999	Mejia et al.	
	41	5954583	09/21/1999	Green	
	42	5991410	11/23/1999	Albert et al.	
	43	5995956	11/30/1999	Nguyen	
	44	6078251	06/20/2000	Landt et al.	
	45	6182214	01/30/2001	Hardjono	
	46	6192222	02/20/2001	Greeff et al.	
	47	6212175	04/03/2001	Harsch	
	48	6219439	04/17/2001	Burger	
	49	6223984	05/01/2001	Renner et al.	
	50	6249212	06/19/2001	Beigel et al.	
	51	6259367	07/10/2001	Klein	
	52	6272562	08/07/2001	Scott et al.	
	53	6285681	09/04/2001	Kolze et al.	
	54	6304613	10/16/2001	Koller et al.	
	55	6307517	10/23/2001	Lee	
	56	6317027	11/13/2001	Watkins	
	57	6325285	12/04/2001	Baratelli	
	58	6366967	04/02/2002	Wagner	
	59	6377176	04/23/2002	Lee	
	60	6420961	07/16/2002	Bates et al.	
	61	6483427	11/19/2002	Werb	
	62	6496595	12/17/2002	Puchek et al.	
	63	6496806	12/17/2002	Horwitz et al.	
	64	6509828	01/21/2003	Bolavage et al.	
	65	6617962	09/09/2003	Horwitz et al.	
	66	6677852	01/13/2004	Landt	
	67	6717516	04/06/2004	Bridgelall	
	68	6903656	06/07/2005	Lee	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/539,431
				Filing Date	August 11, 2009
(Use as many sheets as necessary)				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	3	of	5	Attorney Docket Number	2943AAAB-178

	69	6922558	07/26/2005	Delp et al.	
	70	6963270	11/08/2005	Gallagher, III et al.	
	71	6992567	01/31/2006	Cole et al.	
	72	7026935	04/11/2006	Diorio et al.	
	73	7197279	03/27/2007	Bellantoni	
	74	7268681	09/11/2007	Fitzgibbon	
	75	7269416	09/11/2007	Guthrie et al.	
	76	7375616	05/20/2008	Rowse et al.	
	77	7378967	05/27/2008	Sullivan et al.	
	78	7551081	06/23/2009	Vrba et al.	
	79	2002/0036569	03/28/2002	Martin	
	80	2002/0131595	09/19/2002	Veda et al.	
	81	2003/0007473	01/09/2003	Strong et al.	
	82	2003/0055667	03/20/2003	Sgambaro et al.	
	83	2003/0081785	05/01/2003	Boneh et al.	
	84	2004/0069852	04/15/2004	Seppinen et al.	
	85	2004/0087273	05/06/2004	Pertti1a et al.	
	86	2004/0089707	05/13/2004	Cortina et al.	
	87	2004/0176032	09/09/2004	Kotola et al.	
	88	2004/0179684	09/16/2004	Appenzeller et al.	
	89	2004/0212493	10/28/2004	Stilp	
	90	2004/0232220	11/25/2004	Beenau et al.	
	91	2005/0010750	01/13/2005	Ward et al.	
	92	2005/0036620	02/17/2005	Casden et al.	
	93	2005/0063004	03/24/2005	Silverbrook et al.	
	94	2005/0116813	06/02/2005	Raskar	
	95	2005/0127172	06/16/2005	Merkert Sr.	
	96	2006/0101274	05/11/2006	Merkert et al.	
	97	2006/0156027	07/13/2006	Blake	
	98	2006/0181397	08/17/2006	Limbachiya	
	99	2006/0255129	11/16/2006	Griffiths	
	100	2006/0288101	12/21/2006	Mastrodonato et al.	
	101	2007/0273497	11/29/2007	Kuroda et al.	
	102	2008/0014867	01/17/2008	Finn	
	103	2008/0032626	02/07/2008	Chen	
	104	2008/0094171	04/24/2008	Sawhney	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [2] Applicant's unique citation designation number (optional). [3] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [4] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [5] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [6] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [7] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	4	of	5	Attorney Docket Number	2943AAAB-178

	105	2008/0229400	09/18/2008	Burke		
	106	2009/0315673	12/24/2009	Huang		
	107	2010/0001840	01/17/2010	Kang et al.		

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	108	CN 1307309	08/08/2001	BEIJING KERUIQI TECHNOLOGY DEV		(with English abstract)
	109	EP 0956818	11/17/1999	CITICORP DEV CENTER		
	110	EP 1251448	10/23/2002	TOO MNOGOPROFILNOE PREDPR		
	111	GB 2256170	12/02/1992	BRANDES WILLIAM ROBERT		
	112	GB 2331825	06/02/1999	NEC CORP		
	113	JP 2002-261749	09/13/2002	MATSUSHITA ELECTRIC IND CO LTD		(with English abstract)
	114	KR 2002-0073716	09/28/2002	FIRSTECH INT INC		(with English abstract)
	115	RU 2158444	10/27/2000	AJ DI SISTEMS INK		(with English abstract)
	116	RU 2195020	12/20/2002	MNOGOPROFIL NOE PRED OOO EHLSI		(with English abstract)
	117	WO 97/17683	05/15/1997	ID SYSTEMS INC		
	118	WO 99/56429	11/04/1999	IDENTIX INC		
	119	WO 01/13218	02/22/2001	SIEMENS AG		(with English Abstract)
	120	WO 2004/010373	01/29/2004	BANQUE TEC INTERNAT PTY LTD		
	121	WO 2005/001777	01/06/2005	SCM MICROSYSTEMS GMBH		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	12/539,431
				Filing Date	August 11, 2009
				First Named Inventor	Michael Davis
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	5	of	5	Attorney Docket Number	2943AAAB-178

	122	WO 2006/123316	11/23/2006	KONINKL PHILIPS ELECTRONICS NV		
	123	WO 2007/094868	08/23/2007	MOJIX INC		

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Espacenet

Bibliographic data: CN1307309 (A) — 2001-08-08

Portable recognizer for intelligent anti-fake magnetic card type ID cards

Inventor(s): ZHANG SHUXIN [CN]; XU CHUANXIANG [CN] ± (SHUXIN ZHANG, ; CHUANXIANG XU)

Applicant(s): BEIJING KERUIQI TECHNOLOGY DEV [CN] ± (BEIJING KERUIQI TECHNOLOGY DEVELOPMENT CO., LTD)

Classification: **- international:** ***G06K5/00; G06K7/00; G06K9/00;*** (IPC1-7): G06K5/00; G06K7/00; G06K9/00

- Euro:

Application number: CN20001000720 20000202

Priority number (s): CN20001000720 20000202

Abstract of CN1307309 (A)

The portable recognizer of the present invention includes keyboard, display screen, battery as power source, fingerprint data collector, intelligent IC card reader, magnetic card slot and CPU unit with one embedded low power consumption CPU chip for decode, decompression, fingerprint comparison, automatic recognition, display, etc. The portable ID card recognizer has integral functions of off-line fingerprint collection and comparison, IC card reading, magnetic card reading and personal data browsing.

Last updated: 24.09.2012 Worldwide Database 5.7.44.2; 92p

WAVELYNX EX. 1003, Pg. 1558
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06K 9/00
G06K 5/00 G06K 7/00

[12]发明专利申请公开说明书

[21]申请号 00100720.3

[43]公开日 2001年8月8日

[11]公开号 CN 1307309A

[22]申请日 2000.2.2 [21]申请号 00100720.3

[71]申请人 北京科瑞奇技术开发有限公司
地址 100032 北京市西城区金融街23号平安大厦803室
[72]发明人 张树新 许传祥

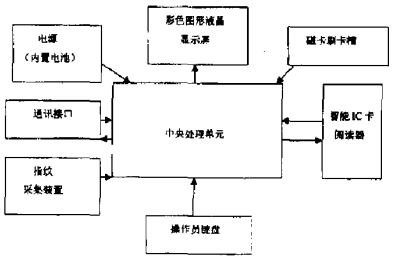
[74]专利代理机构 中国商标专利事务所
代理人 徐小琴

权利要求书1页 说明书6页 附图页数9页

[54]发明名称 便携式智能防伪磁条卡型身份证件识别器

[57]摘要

本发明为一种便携式智能防伪磁条卡型身份证件识别器，包括操作键盘，显 示屏，电源，它还包括指纹采集装置；智能IC卡阅读器；磁卡刷卡槽，用于进行 解密、解压缩和进行指纹比对、全自动识别、显示照片和验卡结果等文字信息的 中央处理单元，该单元包括一低功耗嵌入式CPU芯片。电源采用内置电池供电。提供了集指纹采集、IC卡阅读、磁条阅读、指纹比对、持证人个人信息浏览于 一体的脱机的便携式身份证件识别器。其读取卡内信息方便快捷，安全性高，可 有效的防伪，特别方便外出用户的需要。



ISSN1008-4274

知识产权出版社出版

WAVELYNX EX. 1003, Pg. 1559
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

00·02·02

权 利 要 求 书

1、 一种便携式智能防伪 IC 磁条卡型身份证件识别器，包括输入数据的操作键盘，显示证卡信息的显示屏，电源，其特征在于，它还包括用于采集指纹图像的指纹采集装置；用于读写 IC 卡的智能 IC 卡阅读器；磁卡刷卡槽；仪器控制电路板；仪器控制电路板包括用于进行解密、解压缩和进行指纹比对、全自动识别、显示照片和验卡结果等文字信息的中央处理单元，接口电路，指纹图象提取电路，键盘电路，磁卡阅读电路，中央处理单元包括用于存储数据和程序的通用存储器芯片组，接口电路包括键盘和 IC 卡接口电路，磁卡阅读电路，串行口通讯接口电路 。

2、按照权利要求 1 所述的便携式智能防伪 IC 磁条卡型身份证件识别器，其特征在于，中央处理单元包括一低功耗 3 2 位嵌入式ＣＰＵ芯片。

3、按照权利要求 1 或 2 所述的便携式智能防伪 IC 磁条卡型身份证件识别器，其特征在于，电源采用内置电池供电，并经 DC/IC 变换，产生多种电压的直流输出。

4、按照权利要求 1 所述的便携式智能防伪 IC 磁条卡型身份证件识别器，其特征在于，显示装置采用半反射式彩色图形液晶显示器。

WAVELYNX EX. 1003, Pg. 1560
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

00·04·14

说　明　书

便携式智能防伪磁条卡型身份证件识别器

本发明属于计算机识别领域，涉及采用指纹自动识别、图象压缩、数据加密以及网络通讯功能。特别是一种集指纹采集、IC卡阅读、磁条阅读、指纹比对、持证人个人信息（姓名、年龄、像片等）浏览于一体的脱机的便携式身份证件识别器。

证件的防伪问题一直是困扰着人们和政府的难题。对于许多重要的证件，如身份证、信用卡、护照、机要部门出入证等，对持卡的身份验证是其最主要的功能。由于这些证件对于个人和社会的重要性，也由于现在的证件伪造技术愈来愈高超，这些证件的防伪、防盗用也成为愈来愈迫切的问题。

以往的IC卡内不能存储持卡人的像片、指纹以及简要信息。而现有的IC卡身份证件识别装置，只能阅读IC卡的信息或通过指纹摄取仪，电脑存储识别系统分别完成采集指纹、指纹对比的过程。这些装置不仅占用空间大，能源消耗多，而且不能同时在一个装置内进行阅读IC卡身份证、磁条阅读、采集指纹、指纹对比，显示照片等图像信息和姓名等文字信息。

本发明的发明人已研制出一种《智能防伪IC卡身份证件识别器》（参见专利号ZL 99204693.9）。该仪器虽然能在一个装置内进行阅读IC卡、采集指纹、指纹对比，显示照片等图像信息和姓名等文字信息，但仍然存在仪器体积大，功耗高，不能使用电池供电，不易携带的缺点。

本发明的目的是为了提供一种集指纹采集、IC卡阅读、磁条阅读、指纹比对、持证人个人信息（姓名、年龄、像片等）浏览于一体的脱机的便携式身份证件识别器，其能够方便快捷的读取卡内信息，特别方便外出人员的需要。

根据智能IC卡是一种高密度、高信息含量的便携式文件，可实现证件卡等大容量、可靠性信息存储，并可记录很多附加

WAVELYNX EX. 1003, Pg. 1561
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

说 明 书

的内容，如违章记录，检查记录，培训记录，计划生育记录等及可用机器自动读取的特点，本发明针对识别存储有经过加密和压缩的两枚（多枚）指纹特征数据、像片和有关个人文字信息的IC卡身份证件而设计。它包括输入数据的操作键盘，显示证卡信息的显示屏，电源，其特征在于，它还包括用于采集指纹图像的指纹采集装置；用于阅读IC卡的智能IC卡阅读器；用于磁条信息的磁卡阅读器；仪器控制电路板；仪器控制电路板包括用于进行解密、解压缩和进行指纹比对、全自动识别、显示照片和验卡结果等文字信息的中央处理单元，指纹及图象提取电路，键盘电路，接口电路，磁卡阅读电路，中央处理单元包括用于存储数据和程序的通用存储器芯片组，接口电路包括键盘和IC卡接口电路，磁卡阅读电路，串行口通讯接口电路 。

为了达到使仪器体积小，功能全，便于手持操作的目的，本发明便携式智能防伪 IC 卡型身份证件识别器的中央处理单元包括一低功耗 32 位嵌入式 C P U 芯片。电源采用内置电池供电，并经 DC/IC 变换，产生多种电压的直流（DC）输出。

为了使仪器即使在较弱的光线下也可以显示持卡人的像片和简要信息，显示屏采用半反射式彩色图形液晶显示屏。并可设置按键蜂鸣器提示操作键盘输入的信息确认。

本发明通过硬件结构的设计结合解密、解压缩和进行指纹全自动识别、显示照片和验卡结果等文字信息的软件，由这些软硬件功能模块构成一个便于手持操作，体积小而功能全的智能化IC卡身份证件识别仪器。该仪器具有三强（运算、控制、通讯功能强）一快（仪器验卡速度快）二省（省电—节能、省空间—体积小）的特征。可应用在各种需要准确识别身份的场合如：公安、海关、银行、邮局、考场、宾馆等场所，验证IC卡身份证件的真伪。特别是它可以现场采集持卡人的指纹进行比对，现场读取证件中信息，显示持证人的个人信息和像片，可将卡正面信息以及持证人进行对比；并同时支持IC卡阅读和磁卡阅读，即使在磁条或条码其中一种方式被损坏的情况下，仍可通

WAVELYNX EX. 1003, Pg. 1562
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

说　明　书

过另一种方式读取信息，方便用户选择和使用。因而，本实用新型方便用户可在任何地方和任何时间进行操作，响应了市场对便携式特点的需求，为解决居民身份证，暂住证，军官证，驾驶证，护照等个人身份证件的彻底防伪提供了一种切实可行的装置。

本发明还具备其它功能：

本发明实行模块化开放性的设计，扩展性好，支持用户可编程的多种用途的应用。可以作为制作智能防伪 IC 卡身份证件的指纹采集、特征提取和信息加密、信息编码设备；配置相应的应用软件可进行各种事务的处理、通讯和信息资料的接收、传输和检索等工作，查询统计方便。可提供多层次的数据安全保障，并给予基本的数据保护功能。在物理与电子性方面达到更严格的安全保障。即可脱机使用，又可同时利用网络通讯可快捷有效的查询“黑名单”，可以实现各种方式的黑名单（通缉犯、犯罪嫌疑人）查询（以指纹方式、姓名方式、像片方式等，可有效的防范各种犯罪行为。

下面结合附图详细说明实施例

图 1 为发明的原理框图

图 2 为本发明的操作流程图

图 3 为本发明中央处理单元的 CPU 模块电路原理图

图 4 为本发明中央处理单元的存储器电路原理图

图 5 为本发明采集指纹的电路原理图

图 6 为本发明键盘与 IC 卡接口电路原理图

图 7 为本发明磁卡阅读电路原理图

图 8 为本发明通讯接口电路原理图

图 9 为本发明键盘电路原理图

图 10 为本发明电源电路原理图

图 11 为本发明 IC 卡硬件接口的电路图

图 12 为本发明实体俯视图(外观俯视图)

参见图示:

WAVELYNX EX. 1003, Pg. 1563
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

说　明　书

图 3 为本发明中央处理单元的 CPU 模块电路原理图，其中，芯片 U1 为低功耗 32 位嵌入式 CPU 芯片，采用 32 位 RISC 芯片。31 为 CPU 模块与显示器接口的连接端，32，33 为 CPU 的地址总线和数据总线，34 为 CPU 模块与键盘接口的连接端，35 为 CPU 模块与通讯接口电路的连接端。36 为 CPU 模块与磁条数据输出接口的连接端。

图 4 为本发明中央处理单元的存储器电路原理图，其中，41 为扩展槽，采用 SAMTEG 芯片 。芯片 U2、U3、U4、U5 为（Flash Memory ）作为程序数据存储器，芯片 U6、U7、U8、U9 为 DRAM 通用存储器芯片组。42，43 分别为存储器电路与 CPU 模块的地址总线和数据总线相连的连接端，图 4 的 42，43 分别与图 3 的 32，33 的相应管脚相连。中央处理单元执行指纹特征提取、指纹全自动比对、数据解密和解压缩、逻辑控制和数据通讯等功能。

图 5 为本发明采集指纹的电路原理图。指纹采集装置采用 CMOS 指纹传感器，芯片 U10 为 CMOS 传感器 FPS110。采集的指纹图象数据 51，52 与图 3 的 CPU 模块的地址总线和数据总线 32，33 相连，送 CPU 处理。

图 6 为本发明键盘与 IC 卡接口电路原理图，其中芯片 U11 采用 AT90S4414 单片机，其中，62 为 IC 卡接口，与 IC 卡智能读写器相连。61 为键盘，IC 数据通讯接口，与图 3 的 CPU 模块的 34 相连。63，64 为键盘扫描线。与图 9 的 91，92 相连。

图 7 为本发明磁卡阅读电路原理图。其中，71 为磁卡阅读电路与磁头的连接端，72 为磁条数据输出接口，与图 3 的 CPU 模块的 36 相连。

图 8 为本发明通讯接口电路原理图，其中，81 为通讯接口芯片，两个 RS232C 串行通讯接口，用于与 PC 的串行通信或通过 Modem 连入广域网。其中，81 与图 3 的 CPU 模块的 35 相连。

图 9 为本发明中的键盘电路原理图，操作键盘采用 4X4 矩

WAVELYNX EX. 1003, Pg. 1564
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

说　明　书

阵键盘，由仪器主板上的键盘译码模块扫描和译码键盘输入命令和数据。其中，91，92 与图 6 的 63，64 相连，完成扫描键盘的功能。

图 10 为本发明的电源电路原理图，其中电源采用内置电池供电，并经 DC/DC 变换产生多电压直流（DC）输出。

图 11 为本发明 IC 卡硬件接口电路，其 IC 卡硬件接口与图 6 的 62 端相接。

本发明所用的 IC 卡读卡器，可读 2KB、4KB、8KB、16KB 容量的 IC 卡身份证件，在取得权威机关授权的情况下，可改写 IC 卡身份件。

图 12 为本发明实体俯视图（外观俯视图），其中 121 为指纹采集窗口，122 为显示屏，123 为键盘，124 为插卡处。125 为磁卡刷卡槽。仪器的结构形式为手持式。体积较小，仅占大约 500 多立方米的空间。

本发明的操作过程可参见图 2，持证人将 IC 卡插入插卡处，中央处理单元 CPU 与 IC 卡之间相互认证，读取 IC 卡数据，输出显示 IC 卡数据内容。持证人再将手指在指纹采集窗口按一下，指纹采集装置采集指纹图象，通过应用程序和证卡内的信息进行比较，输出比较结果。本发明验卡时，前后操作过程只花费几秒钟时间，操作非常简便快捷。

如果受验证的两枚手指均已受伤或根本没有指纹（如残疾），可通过反射式液晶屏幕上显示的照片（来自 IC 卡上存放的照片数据）、证卡正面印刷的照片或持卡人相貌三者之间的相互比对来确定卡的真伪，从而避免了在特殊情况下出现的不能正常验卡的问题。

本发明采用内置充电电池，不仅可以手持操作，体积小、而且功能全。操作时间长，充电快。显示直观，非常易于理解和使用，并具有键盘安全化操作的优点。可随意携带到任何地方，机动性不受条件限制，方便了外出人员的使用。

本发明提供了集指纹采集、IC 卡阅读、指纹比对、持证人

WAVELYNX EX. 1003, Pg. 1565
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

00·02·02

说　明　书

个人信息（姓名、年龄、像片等）浏览于一体的脱机的便携式身份证件识别器。其能够通过指纹来识别IC卡身份证件的真伪，并可处理在一张IC卡身份证里面同时存储两枚以上指纹、一幅彩色照片和文字信息的IC卡身份证件。其读取卡内信息能够方便快捷，具有高度的安全性，可有效的防止伪造，特别方便外出用户的需要。

WAVELYNX EX. 1003, Pg. 1566
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

00-02-02

说 明 书 附 图

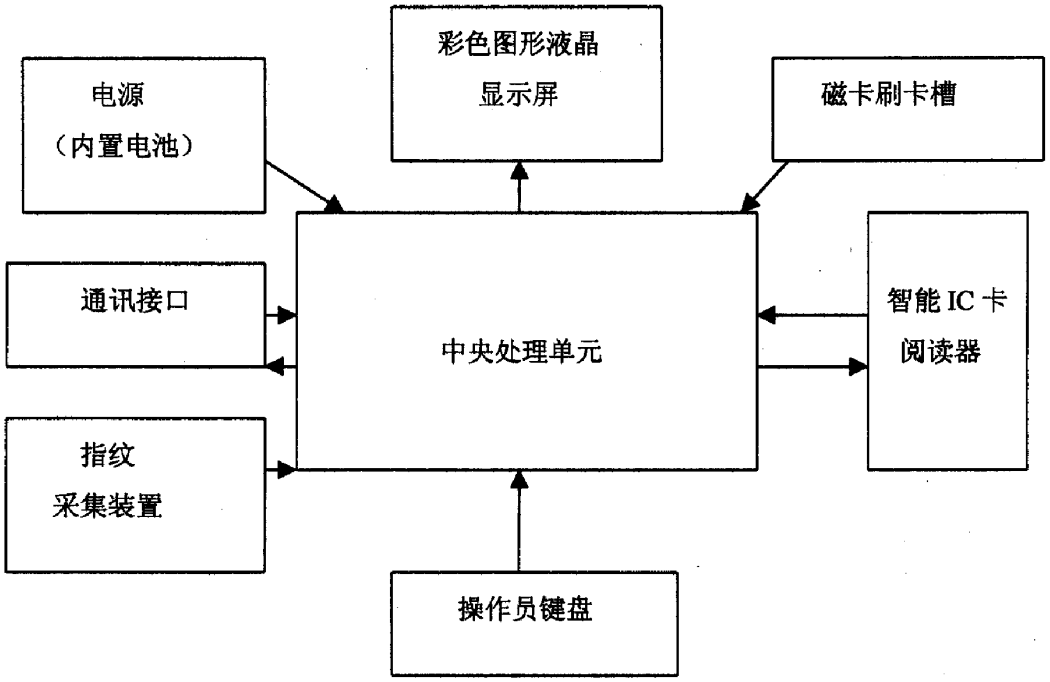


图 1

WAVELYNX EX. 1003, Pg. 1567
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

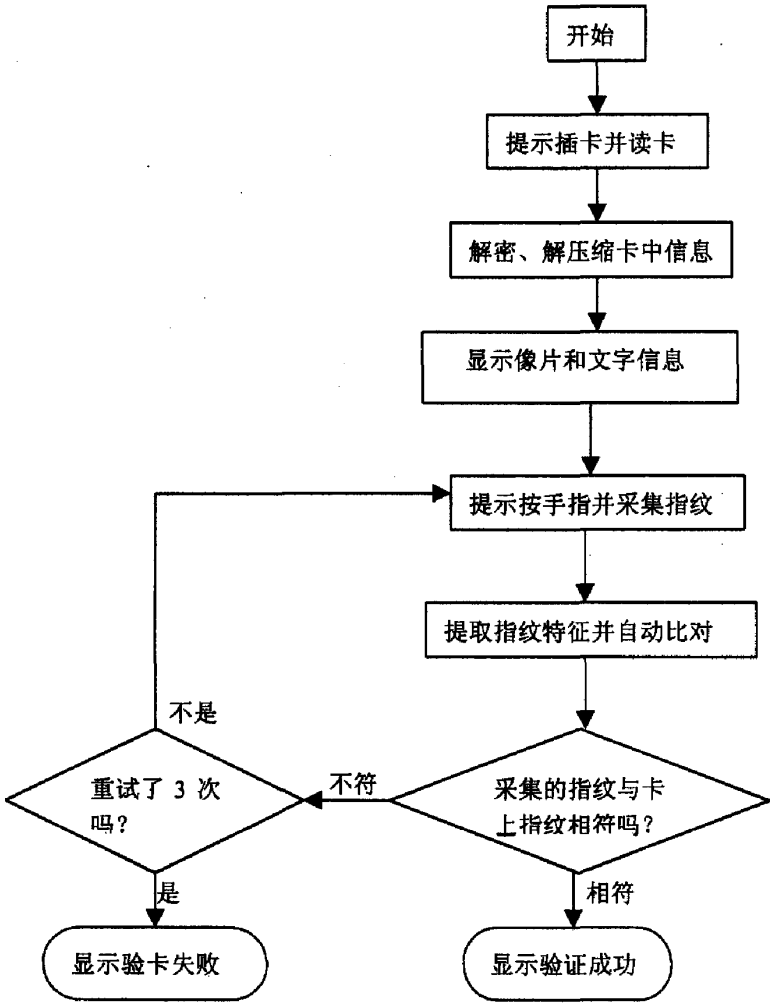


图 2

WAVELYNX EX. 1003, Pg. 1568
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

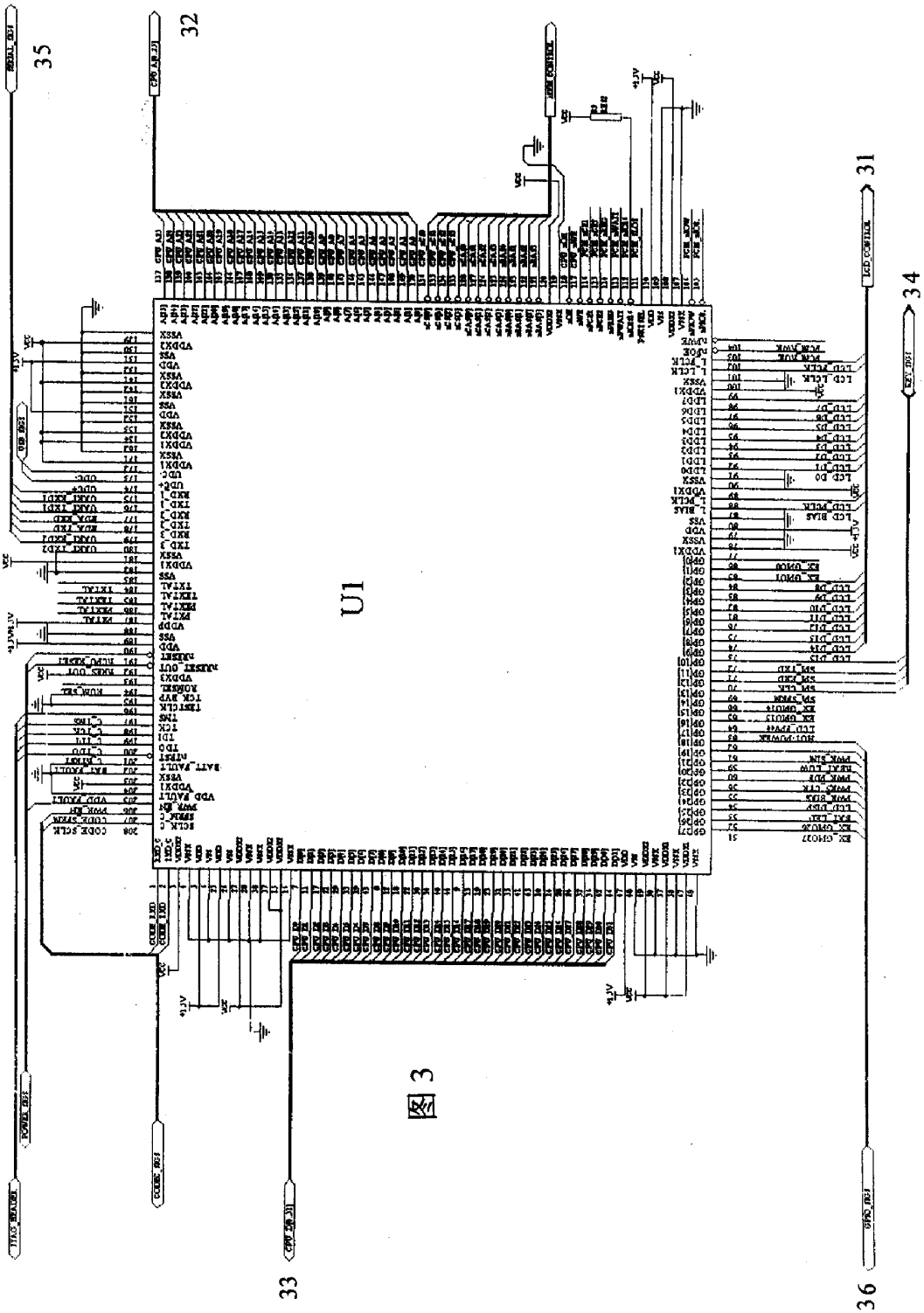


图 3

WAVELYNX EX. 1003, Pg. 1569
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

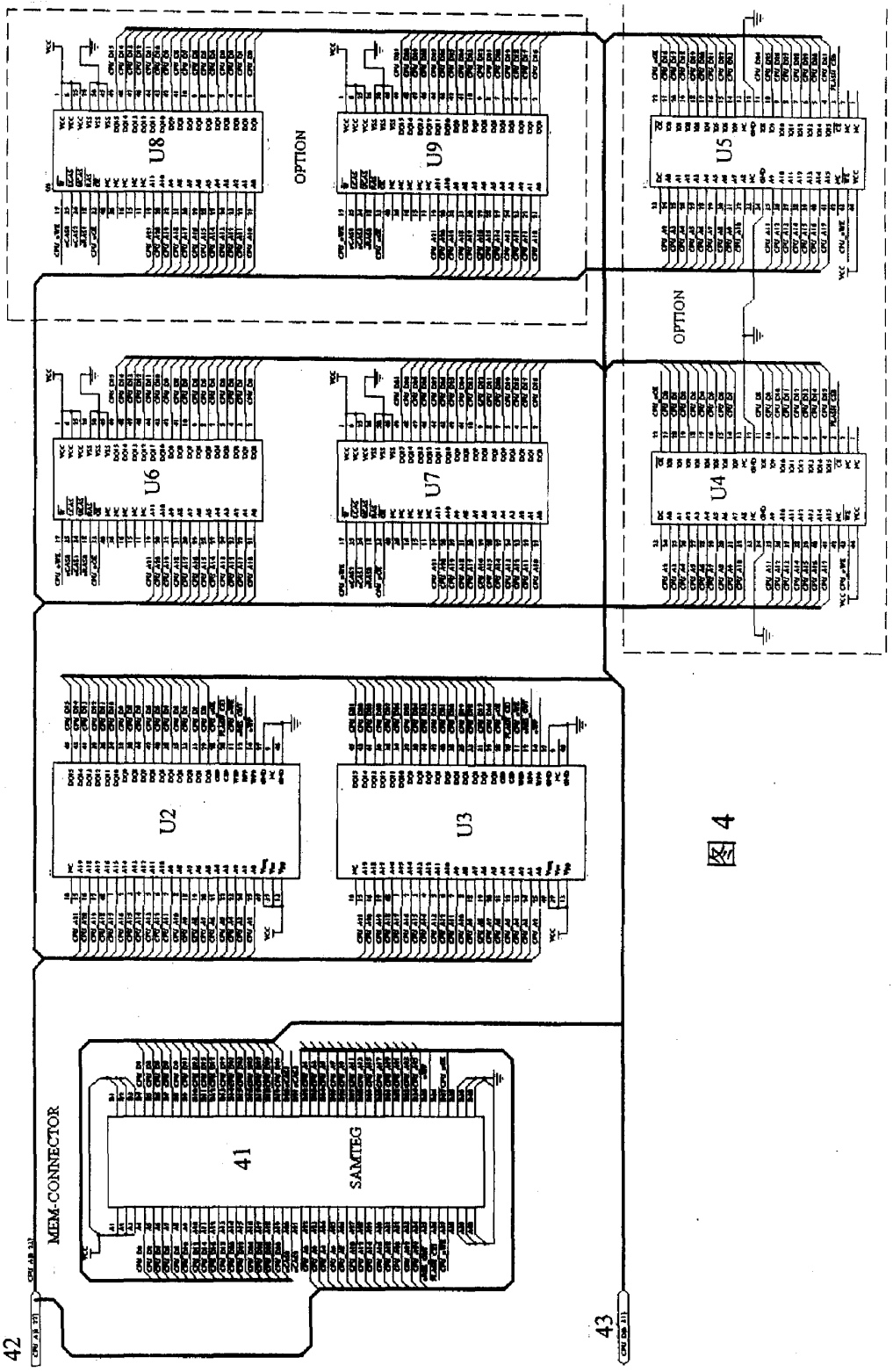


图 4

WAVELYNX EX. 1003, Pg. 1570
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

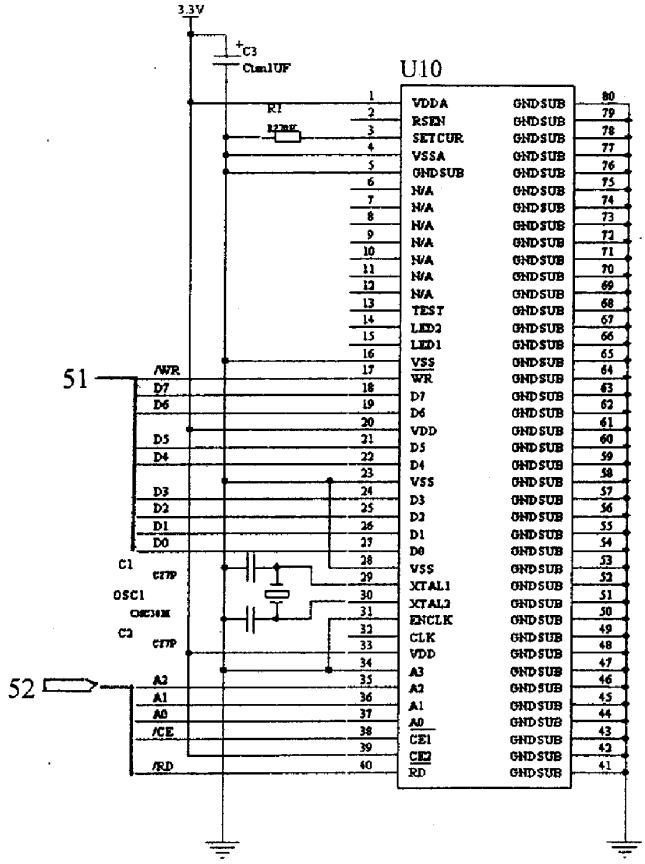


图 5

WAVELYNX EX. 1003, Pg. 1571
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

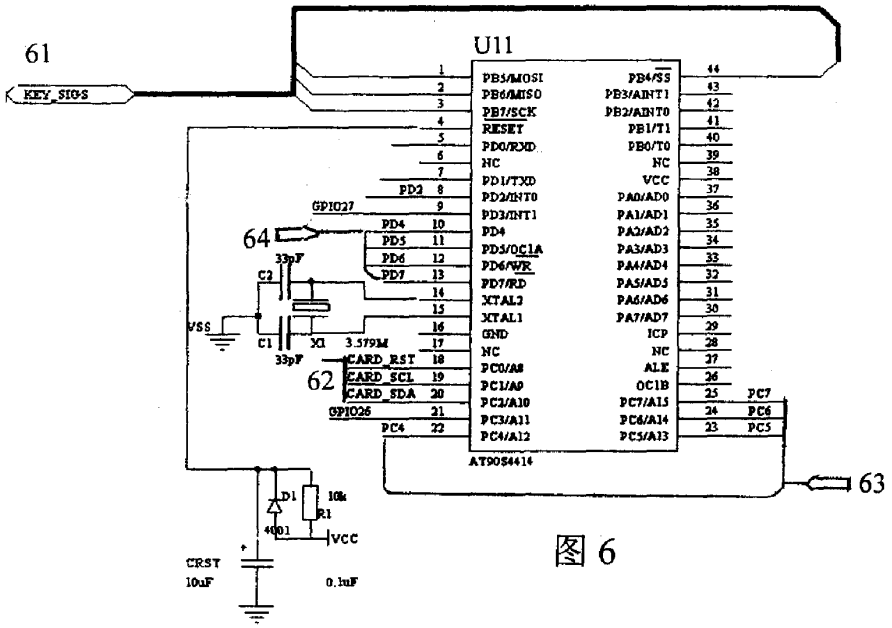


图 6

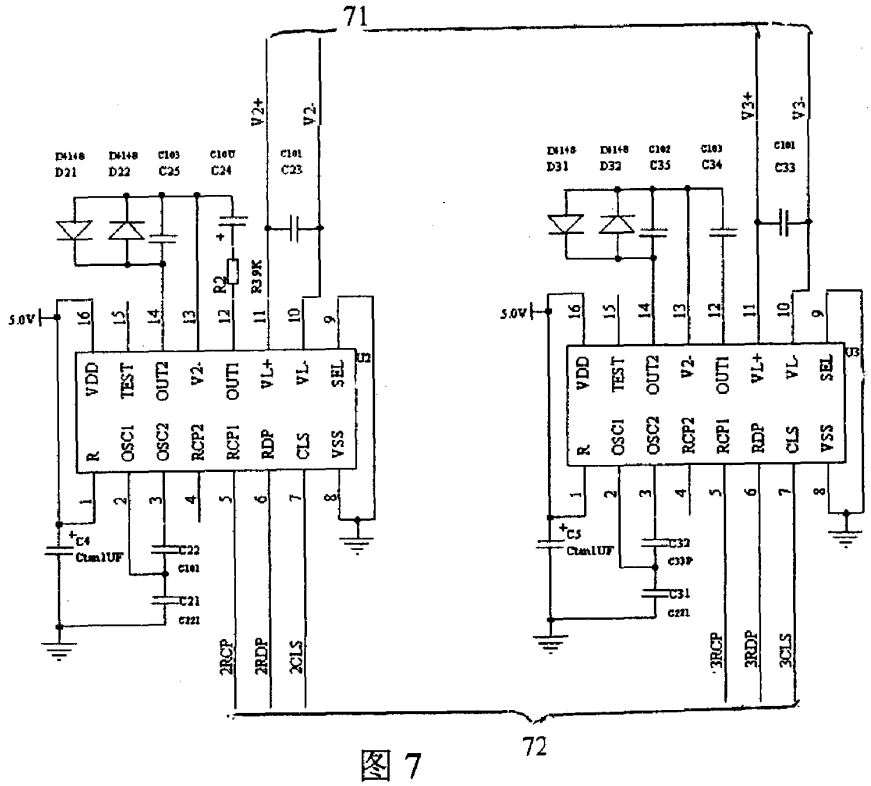


图 7

WAVELYNX EX. 1003, Pg. 1572
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

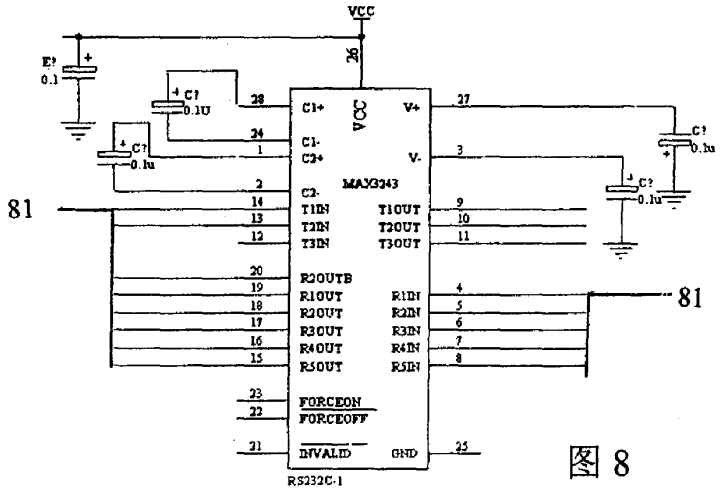


图 8

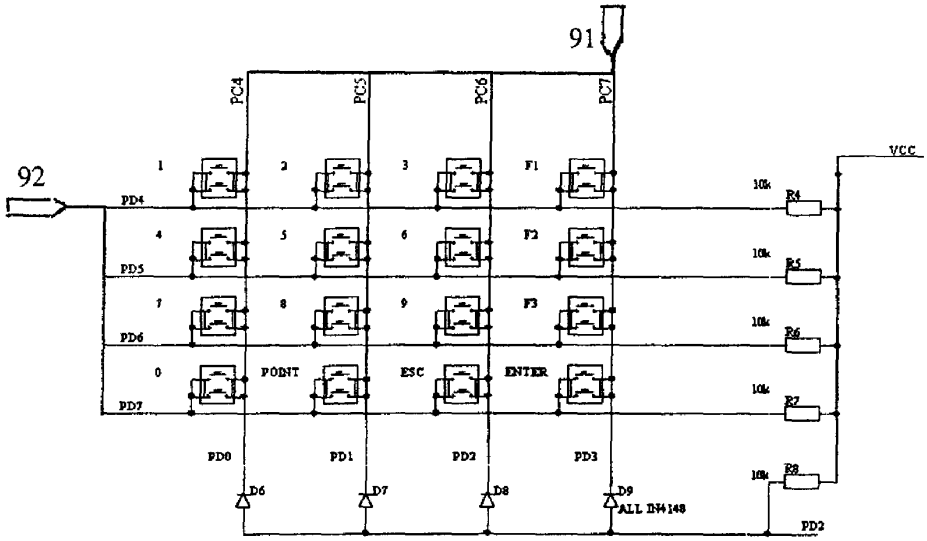


图 9

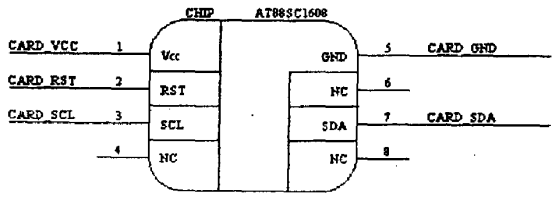


图 11

WAVELYNX EX. 1003, Pg. 1573
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

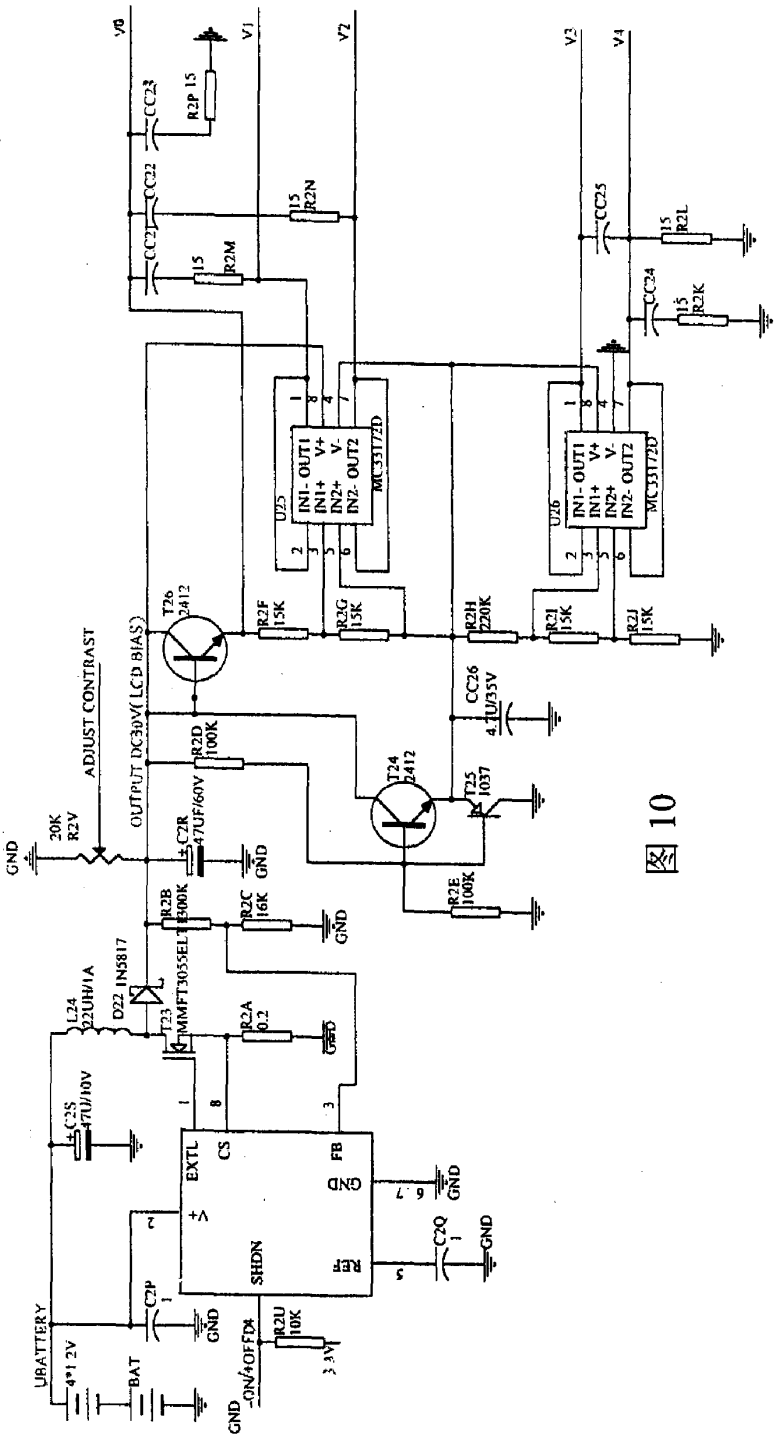


图 10

WAVELYNX EX. 1003, Pg. 1574
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

00.02.02

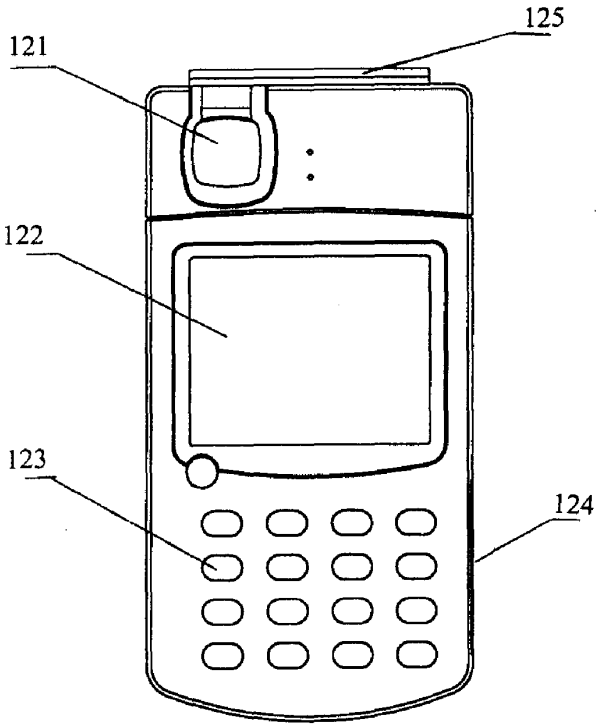


图 12

WAVELYNX EX. 1003, Pg. 1575
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 956 818 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
17.11.1999 Bulletin 1999/46

(51) Int Cl.[6]: **A61B 5/117**, G06K 9/00

(21) Application number: **99201446.4**

(22) Date of filing: **10.05.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **11.05.1998 US 84922 P**

(71) Applicant: **Citicorp Development Center**
Los Angeles, CA 90066 (US)

(72) Inventor: **Shinn, Philip C.,**
Los Angeles, California 90034 (US)

(74) Representative: **Hynell, Magnus**
Hynell Patenttjänst AB,
Patron Carls väg 2
683 40 Hagfors/Uddeholm (SE)

(54) System and method of biometric smart card user authentication

(57) A system and method for authenticating a smart card user (54) at a reader device (64) makes use of an application (58) on a smart card microprocessor (60) on which information fields (56) relating to biometric information for the user and a table of predefined probability of occurrence values for user authentication is stored. The smart card (62) and a biometric sample for the user is presented to the reader device (64), and an application associated with the reader device automatically authenticates the user base on a match level between the stored biometric information and the presented biometric sample according to a desired probability of occurrence value from the stored table. Alternatively, the user (54) is automatically authenticated by an application (58) on the smart card microprocessor (60). The reader device reads the presented biometric sample, automatically presents what is read to the smart card application, and the smart card application then authenticates the user according to the threshold match score from the stored table that corresponds to the desired probability of occurrence value.

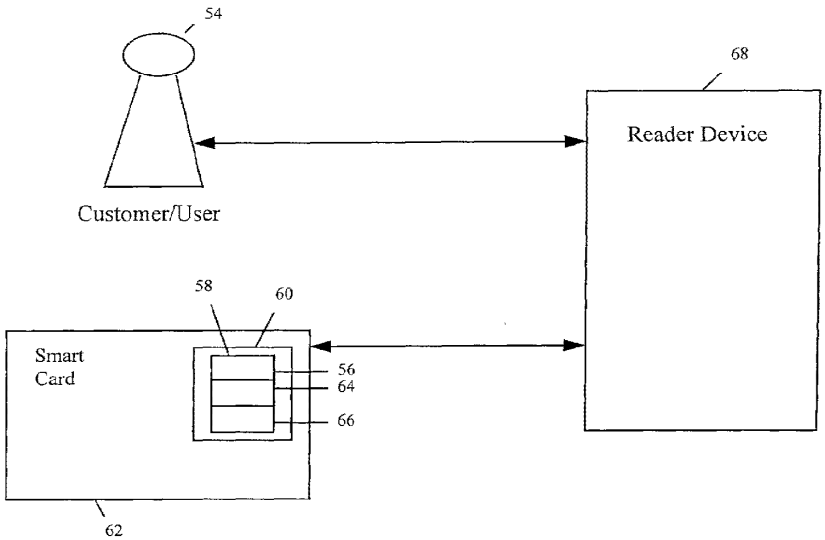


FIG. 5

EP 0 956 818 A1

Printed by Jouve, 75001 PARIS (FR)

WAVELYNX EX. 1003, Pg. 1576
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Description

Cross Reference to Related Applications

[0001] This application claims the benefit of U.S. Provisional Patent Application Serial No. 60/084,922 filed May 11, 1999.

Field of the Invention

[0002] The present invention relates to smart card security and more particularly to a system and method of biometric authentication of a smart card user.

Background

[0003] Authentication is the process by which an entity, such as a financial institution or bank or other type of institution, identifies and verifies its customers or users to itself and itself to its customers or users. Authentication includes the use of physical objects, such as cards and/or keys, shared secrets, such as personal identification numbers (PIN's) and/or passwords, and biometric technologies, such as voice prints, photos, signatures and/or fingerprints. Biometric tasks include, for example, an identification task and a verification task. The verification task determines whether or not the individual claiming an identity is the individual whose identity is being claimed. The identification task determines whether the biometric signal, such as a fingerprint, matches that of someone already enrolled in the system.

[0004] Typically, biometric systems have a common methodology, regardless of their modality, such as fingerprint, face, voice, or the like. A person enrolls by donating some number of samples of the biometric. From these samples, the biometric system creates a model of the particular individual's patterns, which is referred to as a template. When the person attempts to access the system, the application collects new data. In a verification application, the individual claims an identity, and the application retrieves the individual's model from a database and compares the new signal to the retrieved model. The result of this comparison is a match score, which indicates how well the new signal matches the template. The application then compares the match score obtained with a pre-defined threshold and decides whether to allow or deny access to the individual or, for example, to ask the individual for more data.

[0005] Various authentication parameters are used by security systems to verify a valid cardholder and to grant the cardholder access to a secured resource. Information parameters, such as PIN's, can be readily read and processed by a card reader according to a system verification algorithm. However, information can be compromised, so that many authentication systems also require person-unique biometric parameters, such as fingerprints, or retinal images. In such authentication systems, cardholder bio-specimens are stored in digital format in the system computer. During authentication the system obtains the information parameters, for example, from the card, and the biometric parameters from the person and matches both to the system-stored values. For a fingerprint, for example, there are fourteen points and interpoint distances that the biometric reader compares and, depending on the match score, grants or denies access.

[0006] The required match score is a function of a preselected security level and is set by the application designer. However, the image acquisition tolerances, as well as changes in the person's biometric parameter, such as a finger cut on the referenced fingerprint, cause false acceptances, such as accepting an impostor (False Accept or FA), and false rejections, such as rejecting a valid user (False Reject or FR). Manufacturers of biometric readers or application developers provide performance histograms, which are distributions of the empirical number of valid acceptances and valid rejections provided by the reader. To the extent the distributions overlap, there are regions of false rejections of valid users or FR and false acceptance of impostors or FA. In setting the system parameters, application designers attempt to set a threshold authentication match score which balances these tolerances against efficiency for a given application.

[0007] The selected threshold match score is based on the desired probability of occurrence or non-occurrence of a FA and/or FR, and the performance histograms quantify the probability of occurrence of FA and FR. These probabilities are inverse, in that by increasing the threshold score to reduce the Probability of FA or P(FA), the Probability of FR or P(FR) is increased. Conversely, decreasing the threshold to reduce the Probability of FR or P(FR) increases the Probability of FA or P(FA).

[0008] In a given application the selected threshold is coded into the reader software, and system performance is observed. If actual system efficiency is unacceptable due to a False Reject Rate (FRR) that is too high, the threshold score is reduced, and if unacceptable due to a False Accept Rate (FAR) that is too high, the threshold is increased. Each time the threshold score changes, it must be recoded into the reader system software. Similarly, with each new reader model or new release, the threshold score must be changed in accordance with the new model histograms and possibly changed again following actual performance evaluation. Each re-coding of the threshold value generally requires a new system software release, together with the time and labor required to install the new software.

Summary of the Invention

[0009] It is a feature and advantage of the present invention to provide a system and method of biometric smart card user authentication which automatically ad-

WAVELYNX EX. 1003, Pg. 1577
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

justs the probability of occurrence or non-occurrence of false acceptance of an impostor and false rejection of a valid user without the necessity of reprogramming the reader system software.

[0010] It is a further feature and advantage of the present invention of provide a system and method of biometric smart card user authentication in which the performance of the biometric technology is independent of where the system positions the threshold for false acceptance and false rejection.

[0011] It is another feature and advantage of the present invention to provide a system and method of biometric smart card user authentication which makes the card application more secure, thereby reducing the risk of fraudulent or unauthorized use and allowing for higher-value applications

[0012] It is an additional feature and advantage of the present invention to provide a system and method of biometric smart card user authentication which simplifies application design requirements by putting the user's biometric template on the card, thereby eliminating or greatly reducing network traffic.

[0013] It is still another feature and advantage of the present invention to provide a system and method of biometric smart card user authentication which enhances security and privacy by eliminating the necessity of transmitting the user's biometric template around to different locations where it is needed.

[0014] It is a still further feature and advantage of the present invention to provide a system and method of biometric smart card user authentication which allows application designers to set operating thresholds as tightly or as loosely as is appropriate for the particular risk involved.

[0015] It is also a feature and advantage of the present invention to provide a system and method of biometric smart card user authentication with a flexible architecture format for storing biometrics on the smart card that is independent of application or biometric methodology or vendor.

[0016] It is still an additional feature and advantage of the present invention to provide a system and method of biometric smart card user authentication which supports different methods, vendors, and releases, and allows for flexibility of application deployment.

[0017] It is another feature and advantage of the present invention to provide a system and method of biometric smart card user authentication in which the user is automatically authenticated by an application on the smart card.

[0018] It is an additional feature and advantage of the present invention to provide a method and system of biometric smart card user authentication in which the customer's use of the smart card in a transaction ties the customer undeniably to the transaction and makes the transaction non-reputiatable.

[0019] To achieve the stated and other features, advantages and objects of the present invention, the system and method for authenticating a smart card user at a reader device of an embodiment of the present invention includes storing information fields for the user on the smart card relating to biometric information for the user, also referred to as a biometric template. The biometric template includes at least one model of biometric patterns for the user, such as the user's voice print, photograph, signature, fingerprint, hand geometry, retinal image or iris scan. The information fields also include a table of pre-defined probability of occurrence values for user authentication, as well as personal data for the user, identification of a biometric system, and a hashed data field. The information fields are stored in an application on a microprocessor of the smart card.

[0020] In an embodiment of the present invention, storing the information fields relating to the table of pre-defined probability of occurrence values involves automatically assigning a probability of occurrence value to each of a plurality of pre-defined range limit values, which are automatically identified for each of a plurality of value ranges of biometric reader device match scores. Identifying the range limit values involves automatically tabulating a performance histogram distribution of biometric reader device match scores for false acceptance of an impostor and false rejection of a valid user into a plurality of value ranges. Tabulating the performance histogram distribution involves automatically quantifying the performance histogram into discrete levels of biometric reader device match scores and automatically assigning the probability of occurrence value for each of the discrete levels of the biometric reader device match scores.

[0021] In an embodiment of the present invention, the smart card, together with a biometric sample for the user, are presented to the reader device, which is associated with a terminal, such as at least one of an area access terminal, a computer network terminal, a computer access terminal, a stored value terminal, a monetary access terminal, a PBX terminal, a long distance terminal, a personal computer, a laptop computer, a personal digital assistant, a public internet terminal, and an automated teller machine. The presented biometric sample is, for example, at least one of a voice print, photograph, signature, fingerprint, hand geometry, retinal image, and an iris scan.

[0022] In an embodiment of the present invention, the user is automatically authenticated by the reader device based at least in part on a match level between the stored biometric information and the presented biometric sample according to a desired probability of occurrence value from the stored table. The desired probability of occurrence value is pre-selected by pre-defining a desired probability of occurrence value for false acceptance of an impostor and false rejection of a valid user and pre-defining an instruction set which directs the reader device to look to the stored table of probability of occurrence values for a false acceptance of an impostor and false rejection of a valid user threshold match score

WAVELYNX EX. 1003, Pg. 1578
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

corresponding to the desired probability of occurrence value. The user authentication is performed by an application associated with the reader device and residing on the reader device and/or the terminal.

[0023] Alternatively, in an embodiment of the present invention, in order to provide enhanced security, the user is automatically authenticated by an application on the smart card. For example, the reader device reads the presented biometric sample and automatically presents what is read by the reader device to the smart card application. The smart card application then authenticates the user according to the threshold match score from the table on the smart card application that corresponds to the desired probability of occurrence value.

[0024] Additional objects, advantages and novel features of the present invention will be set forth in part in the description which follows, and in part will become more apparent to those skilled in the art upon examination of the following or may be learned by practice of the invention.

Brief Description of the Drawings

[0025]

Fig. 1 is a table which illustrates examples of types of data used in measuring biometrics performance for an embodiment of the present invention;

Fig. 2 shows a sample biometric reader device performance histogram for an embodiment of the present invention;

Fig. 3 is a table which illustrates four possible outcomes of a single biometric reader device trial for an embodiment of the present invention;

Fig. 4 is a diagram which illustrates an example of a receiver operating characteristic (ROC) curve for an embodiment of the present invention;

Fig. 5 is a flow chart which shows somewhat schematically an overview of the key components and the flow of information between the key components for an embodiment of the present invention;

Fig. 6 is a table which illustrates examples of the type of data stored on the smart card for an embodiment of the present invention;

Fig. 7 is a table which shows a sample probability look-up table for an embodiment of the present invention; and

Fig. 8 is a flow chart which provides further detail regarding the process of authenticating a user through match scoring of a sample biometric obtained from the user by a biometric reader device for an embodiment of the present invention.

Detailed Description

[0026] Referring now in detail to an embodiment of the present invention, an example of which is illustrated in the accompanying drawings, a number of methods can be used to quantitatively measure biometrics performance. Fig. 1 is a table which illustrates examples of types of data used in measuring biometrics performance for an embodiment of the present invention. The types of data include, for example, performance histogram 2, False Accept Rate (FAR) and False Reject Rate (FRR) 4, Equal Error Rate (EER) 6, Failure to Acquire (FTA) 8, and "d'" and Receiver Operating Characteristic (ROC) plots 10.

[0027] A basic way to look at data for quantitatively measuring the performance of biometrics is to inspect the performance histogram 2. Each time a trial is performed, the system returns a match score which is plotted in the histogram 2. Fig. 2 illustrates a sample biometric reader device performance histogram for an embodiment of the present invention. The histogram 2 has the match score 12 on the x-axis 14, from low scores 16 toward the left side of the histogram to high scores 18 toward the right side of the histogram. The number of cases attempted 20 is shown on the y-axis 22 of the histogram 2. Valid users 24 have higher match scores 18 and are shown on the right side of the histogram 2. Distributions vary from device to device, but are commonly normally distributed as bell curves 26 and 28. Impostors 30 have lower scores 16 and are shown on the left side of the histogram 2. Note also that there are usually fewer impostors 30 than valid users 24.

[0028] Referring further to Fig. 2, the vertical line on the histogram, which separates the two distributions of scores 26, 28, is known as the threshold 32. If a user scores higher than the threshold 32, the user is accepted, but if the user scores lower than the threshold, the user is rejected. There are four possible outcomes of a single trial. Fig. 3 is a table with illustrates the four possible outcomes of a single biometric reader device trial for an embodiment of the present invention. The four possible outcomes include, for example, Correct Accept 34 of a customer, Correct Reject 36 of an impostor, False Accept or FA 38 of an impostor, and False Reject or FR 40 of a customer. The percentage of cases in the False Accept or FA 38 outcome is called the False Accept Rate (FAR), and the percentage of cases in the False Reject or FR 40 outcome is called the False Reject Rate (FRR).

[0029] Referring again to Fig. 2, if the threshold 32 is repositioned toward the left side of the histogram 2, fewer FR's 40 occur, but more FA's 38 occur. If the threshold 32 is repositioned toward the right side of the histogram 2, more FR's 40 occur, but fewer FA's 38 occur. This is the essential tradeoff made in the context of an application for an embodiment of the present invention. An important aspect of an embodiment of the present invention is that the system and method of the present invention automatically moves the threshold, and the performance of the biometric technology is independent of where the application positions the threshold 32.

[0030] The system and method for an embodiment of

WAVELYNX EX. 1003, Pg. 1579
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

the present invention moves the threshold 32 according to the objectives of greater security or rejecting fewer customers. Referring likewise to Fig. 2, if the objective is greater security, the threshold 32 is moved to a higher position. If the objective is to reject fewer customers, the threshold 32 is moved to a lower position. Therefore, comparing a system which has, for example, a stated performance level of 1 percent FAR and 10 percent FRR with another system that has, for example, a performance level of 2 percent FAR and 8 percent FRR is analogous to comparing apples with oranges.

[0031] Different organizational constituencies typically have different perspectives of the FRR and FAR. For example, a security professional may prefer to know what the FRR will be if the FAR is set to 0 percent, while a marketing professional may wish to know what the FAR will be if the FRR is set to 0 percent. The number that is disposed in the middle is the Equal Error Rate (ERR). To address the aspect of movable thresholds, another method of quoting performance is the EER. Referring further to Fig. 2, to find the EER, the threshold 32 is set so that the percentage of FAR equals the percentage of FRR, and the overall error is calculated. For example, if the threshold 32 is set so that 5 percent of valid users 24 are rejected and 5 percent of impostors 30 are accepted, the overall EER is 5 percent. This is the outcomes table of a 5 percent EER.

[0032] Another measure of biometrics performance is called Failure to Acquire (FTA) 8, which is the failure of the system to find a signal to analyze. For example, in the fingerprint area, this is known as the 'presentation problem.' If a user does not place the user's finger on the scanner with the right orientation, or if the user moves the user's finger while the system is scanning, the resulting image cannot be processed. Likewise, in a speech system, if the user does not speak loudly enough, or if there is line noise or a bad connection, the system can fail to find the words. In a face verification system, the system may not be able to find a head in the proper frame it expects, and hence fails to acquire the photo. FTA 8 is often a result of human factor problems, mainly due to the amount of training a user may have or the amount of work a user must do to make the biometric work.

[0033] A numerical description of the degree of separation of two distributions, such as the scores of the valid users 24 and the scores of the impostors 30, known as "d'," is available from statistical decision and signal detection theory, and is related to the Neyman-Pearson equations describing distributions. It is defined according to the equation:

$$d' = (m2 - m1)/\mathrm{sqrt}\,[\,sd1^2 + sd2^2)/2]$$

in which "d'" is equal to the difference between the means of the distributions divided by the square root of the average of the squares of the standard deviations of the distributions.

[0034] Fig. 4 is a diagram which illustrates an example of a receiver operating characteristic (ROC) curve 42 for an embodiment of the present invention. Referring to Fig. 4, the Probability of False Reject or P(FR) 44 is plotted on the y-axis 46, and the Probability of False Acceptance or P(FA)) 48 is plotted on the x-axis 50. As previously mentioned, there is a tradeoff by moving the threshold, for example, higher and rejecting more valid users 23 but also keeping out more impostors 30. This tradeoff is shown as the ROC curve 42. In the ROC curve 42, points near the origin (0, 0) 52 represent operating the biometric with some FA 38 and FR 40, whereas points at the ends of the line represent thresholds which are set very high or very low. For example, the threshold can be set high, such that P(FA) 48 is low and P(FR) 44 is high, or the threshold can be set low, such that P(FA) 48 is high while P(FR) 44 is low.

[0035] Fig. 5 is a flow chart which shows somewhat schematically the key components and the flow of information between the key components for an embodiment of the present invention. Referring to Fig. 5, the system and method for biometric authentication of a smart card user 54 for an embodiment of the present invention involves storing certain information fields 56 in an application 58 on a microprocessor 60 embedded in the smart card 62, along with a biometric sample 64 itself. The information fields 56 include system identification and personal data, as well as a hashed data field, which is decoded by the system during the authentication process to certify the integrity of the information parameters.

[0036] Referring further to Fig. 5, additionally, the application 58 on the smart card 62 includes a probability look-up table 66 which quantifies a reader device performance histogram distribution into discrete levels of match score 12 and assigns a corresponding probability factor to each level for both false acceptances of impostors 30 and false rejections of valid users 24. The system reader device 68 is programmed with a desired Probability of False Acceptances or P(FA)'s 48 and False Rejections or P(FR)'s 44. The system reader 68 is also programmed with an instruction routine that tells the system signal processor to look to the probability look-up table 66 on the card 62 to determine the false acceptances or false rejections threshold match score corresponding to the desired probability factor, to be used for authentication.

[0037] An embodiment of the present invention provides an architecture which allows flexibility in application design. Since application requirements vary in terms of risk, user populations, channel properties and cost, the system and method for an embodiment of the present invention supports a wide range of these properties. Biometric technology provides a type of security that is qualitatively different from that provided by token-based methods and information based methods. Token based methods make use of something that a user has,

WAVELYNX EX. 1003, Pg. 1580
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

such as the card itself, and information-based methods utilize something that the user knows, such as a PIN or password. Biometric technology for an embodiment of the present invention can be used in addition to these other methods or by itself.

[0038] In embodiment of the present invention, the use of biometric technology in conjunction with the smart card 62 makes the card application 58 more secure, thereby reducing the risk of fraudulent or unauthorized use. This allows for the implementation of higher-valued applications. Further, such use of biometric technology provides for non-repudiation of a transaction by the user 54 using the user's smart card 62, so the user cannot deny a transaction performed by the user with the smart card. In other words, use of biometric technology in conjunction with the smart card 62 undeniably ties the user 54 to use of the smart card by the user. In addition, by putting the biometric template 64 on the card 62, application design requirements are simplified, since network traffic is eliminated or greatly reduced. This also enhances security and privacy, since it is unnecessary to transmit the template 64 around to different locations where it is needed.

[0039] The system and method for an embodiment of the present invention has numerous applications, such as secure area access, computer network and computer access, stored value or other monetary access, PBX and long distance access. Each of such applications has different requirements in terms of risk, environment, user, channel and cost. In terms of risk, a transaction which, for example, transfers a million dollars to a numbered Swiss bank account has a higher risk than one which simply returns a user's bank account balance. Gaining access, for example, to a nuclear weapons facility or to war plans or lists of secret agents carries a greater risk than gaining access to an officer's club or DISNEY WORLD. An objective of the application designer is to set application operating thresholds as tightly or as loosely as is appropriate for the particular risk involved.

[0040] In terms of environment, an office environment is different, for example, from an outdoor setting in a public space or a freezing border crossing station. While a face verification system works well, for example, in an office environment, it may not work in a public space where the lighting and background is uncontrolled. Likewise, a hand geometry unit will not work well at the freezing border station, unless heated in some way, but a speaker verification system may work. In regard to the user, if a user uses a particular system frequently, the user soon becomes habituated to the system. Since human factors are an important part of overall system performance, a habituated user typically obtains better system performance than an unhabituated user on any given biometric. Some biometric methods are easier to learn and faster to use than others, so the type of user that is anticipated is an important factor in the selection and deployment of a biometric.

[0041] In terms of channel, some biometrics are more appropriate than others, depending on the channel of use. For example, for long distance or cell phone access, speaker verification is more natural and efficient than, for example, fingerprinting. Secure area access method choice depends on the environment, but signature verification may be more difficult than a camera based method, given the fact that the user may be carrying packages or the like and standing, or the user may be in a wheelchair. However, for a point of sale terminal, if a signature is required in a credit card transaction anyway, and if the merchant is moving to a paper-less business and the terminal has a pressure sensitive tablet for signature capture, then signature verification may be the most appropriate biometric method.

[0042] Other channels include, for example, the personal computer (PC) at home. Since many people only have one phone line into their home, deploying voice authentication may be cumbersome. However, a less cumbersome method may be a camera based method, since people may have cameras for other purposes, such as video teleconferencing. Other channels include, for example, laptop, personal digital assistant (PDA), public internet terminals, automated teller machines (ATM's), vehicles, and the like.

[0043] In terms of cost, there are a number of determinants of cost of a biometric, including the cost of enrollment, such as workstations, user time and monitoring, if supervised. Other cost factors include, for example, the cost of an access trial, such as user time, hardware and software and operations costs amortized over the number of verifications in the expected duration of the system, and the cost of storing the templates, such as the size of the template divided by cost of storage. To illustrate an example of the range of costs, a speaker verification system can be deployed for a telephone network that costs approximately $5,000 per channel for a processor capable of performing up to 5 verifications a minute. If the system performs 300 verifications an hour, 24 hours a day, 7 days a week, 360 days a year, after 3 years when the system is presumed obsolete, the cost per verification is about 6 cents per hundred verifications.

[0044] On the other hand, to illustrate another example of the range of costs, an iris scanner at a secure room portal might also cost about $5,000, but traffic through the portal might only be 30 verifications an hour or less, so the cost per verification for the iris scanner is proportionally greater than for speaker verification. As for template size, a hand geometry unit requires only 9 bytes of storage per template, whereas some fingerprint units and voice units require upwards of a kilobyte per template. Since memory costs on smart cards are not inexpensive, and the amount of time it takes to transfer the data off the card, in the case of matching template to signal off the card, is proportional to the size of the template, template size is an important consideration.

[0045] In an embodiment of the present invention, a

WAVELYNX EX. 1003, Pg. 1581
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

smart card parameter protocol mandates that certain information fields 56 are stored on the card 62, in addition to the biometric sample 64 itself. These information fields 56 include system identification and personal data, as well as a hashed data field, which is decoded by the system during the authentication process to certify the integrity of the information parameters. Fig. 6 is a table which illustrates examples of the type of data stored on the smart card 62 for an embodiment of the present invention.

[0046] Referring to Fig. 6, the content of the first six fields includes, for example, method 70, vendor 72, release 74, template 64, last updated 78, and first enrolled 80. The method field 70 relates to the biometric technology employed, such as fingerprint. The vendor field 72 identifies the particular vendor, such as SONY. The release field 74 specifies a release number, such as 1.0. The template field 64 is the particular template, and the last updated and first enrolled fields 78, 80 indicate dates. Referring further to Fig. 6, the hash value 82 is a value which is arrived at by hashing everything in the record. This can be transmitted elsewhere to authenticate the validity of the template 64.

[0047] Another aspect of an embodiment of the present invention is that the card 62 also includes a probability look-up table 66 which quantifies the reader device performance histogram distribution into discrete levels of match score, such as 200, 300, 400, and so on, and assigns a corresponding probability factor to each level. Fig. 7 is a table which shows a sample probability look-up table 66 for an embodiment of the present invention. Referring to Fig. 7, the probability look-up table 66 includes an array of threshold values that are interpreted by the application 58. For example, for a False Accept Rate or FAR of less than 1 in 100, the match value between the template 64 and the presented signal must be greater than 200. Alternatively, for a False Reject Rate or FRR of less than 1 in one million, a threshold value of 400 is used. This is done for both FA 38 and FR 40.

[0048] In an embodiment of the present invention, the system reader 68 is programmed with a desired P(FA) 48 or P(FR) 44 rather than with a fixed threshold value. The system reader 68 is also programmed with an instruction routine that tells the system signal processor to look to the probability look-up table 66 on the card 62 to determine the desired probability factor's corresponding FA 38 or FR 40 threshold match score to be used for authentication. This aspect reduces the cost of new system releases, since the application software may remain the same and only the cards have to be re-programmed, instead of both the system and the cards as in the prior art. In addition, the cards may be programmed for personalized authentication, for example, at either a higher or lower security level, on an individual basis, instead of one value fits all.

[0049] In an embodiment of the present invention, the user 54 is authenticated through match scoring of a sample biometric obtained from the user by the biometric reader device 68. Fig. 8 is a flow chart which provides further detail regarding the process of authenticating a user through match scoring of a sample biometric obtained from the user by a biometric reader device for an embodiment of the present invention. At S1, a biometric template 64 for the user 54 is stored in an application 58 on a microprocessor 60 of the smart card 62, along with information fields 56, including system identification and personal data for the user. At S2, a look-up table 66 based on a tabulation of performance histogram distribution of biometric reader device match scores for false acceptance or FA 38 and false rejection or FR 40 into value ranges, with each value range identified by a range limit value and each range limit value assigned a corresponding probability of occurrence value P(FA) 48 and P(FR) 44, is also stored on the smart card application 58.

[0050] Referring further to Fig. 8, at S3, the user 54 presents the smart card 58, along with a new biometric sample for the user, to the biometric reader device 68 pre-programmed with a desired probability of occurrence value and with an instruction set that commands the reader device to look to the look-up table 66 on the card 58 for the range limit value associated with the desired probability to be used for authentication of the user. At S4, the reader device 58 compares the new biometric sample for the user 54 with the user's biometric template 64 stored on the smart card 62, identifies the range limit value associated with the desired probability of occurrence value, and authenticates the user on the basis of the identified range limit value.

[0051] It is clear that there is no 'one biometric fits all' for every application, nor is there one operating threshold that is appropriate for all applications. An embodiment of the present invention provides a flexible architecture format for storing biometrics on smart cards that is independent of application or biometric methodology or vendor. In an embodiment of the present invention, threshold values are no longer 'hardwired' in a specific application to a specific method, vendor and specific release. The same architecture applies no matter what the risk, vendor, biometric method or release. Thresholds and methods are determined, and probability density functions of various vendors, methods and releases are derived in order to fill in the threshold values. Thus, an embodiment of the present invention supports different methods, vendors and releases, and allows for flexibility in application deployment.

[0052] Various preferred embodiments of the present invention have been described in fulfillment of the various objects of the invention. It should be recognized that these embodiments are merely illustrative of the principles of the present invention. Numerous modifications and adaptations thereof will be readily apparent to those skilled in the art without departing from the spirit and scope of the present invention. Accordingly, the invention is limited only by the following claims.

WAVELYNX EX. 1003, Pg. 1582
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Claims

1. A method of authenticating a smart card user at a reader device, comprising:

   storing information fields for the user on the smart card relating to biometric information for the user and a table of pre-defined probability of occurrence values for user authentication;
   presenting the smart card and a biometric sample for the user to the reader device; and
   automatically authenticating the user based at least in part on a match level between the stored biometric information and the presented biometric sample according to a desired probability of occurrence value from the stored table.

2. The method of claim 1, wherein storing the information fields relating to the biometric information for the user further comprises storing a biometric template for the user.

3. The method of claim 2, wherein storing the biometric template further comprises storing at least one model of biometric patterns for the user selected from a group of biometric patterns consisting of voice print, photograph, signature, fingerprint, hand geometry, retinal image, and iris scan.

4. The method of claim 1, wherein storing the information fields relating to the table of pre-defined probability of occurrence values for user authentication further comprises automatically assigning a probability of occurrence value to each of a plurality of pre-defined range limit values.

5. The method of claim 4, wherein automatically assigning the probability of occurrence values further comprises automatically identifying the range limit values for each of a plurality of value ranges of biometric reader device match scores.

6. The method of claim 5, wherein automatically identifying the range limit values further comprises automatically tabulating a performance histogram distribution of biometric reader device match scores for false acceptance of an impostor and false rejection of a valid user into the plurality of value ranges.

7. The method of claim 6, wherein automatically tabulating the performance histogram distribution further comprises automatically quantifying the performance histogram distribution into discrete levels of the biometric reader device match scores.

8. The method of claim 7, wherein automatically tabulating the performance histogram distribution further comprises automatically assigning the probability of occurrence value for each of the discrete levels of the biometric reader device match scores.

9. The method of claim 1, wherein storing the information fields further comprises storing personal data for the user on the smart card.

10. The method of claim 1, wherein storing information fields further comprises storing information related to identification of a biometric system on the smart card.

11. The method of claim 1, wherein storing the information fields further comprises storing a hashed data field on the smart card.

12. The method of claim 1, wherein storing the information fields further comprises storing the information fields in an application on the smart card.

13. The method of claim 12, wherein storing the information fields in the application further comprises storing the information fields in an application on a microprocessor of the smart card.

14. The method of claim 1, wherein presenting the smart card further comprises presenting the smart card to the reader device associated with a terminal.

15. The method of claim 14, wherein the terminal further comprises at least one of an area access terminal, a computer network terminal, a computer access terminal, a stored value terminal, a monetary access terminal, a PBX terminal, a long distance terminal, a personal computer, a laptop computer, a personal digital assistant, a public internet terminal, and an automated teller machine.

16. The method of claim 1, wherein presenting the biometric sample further comprises presenting the biometric sample to the reader device associated with a terminal.

17. The method of claim 16, wherein the terminal further comprises at least one of an area access terminal, a computer network terminal, a computer access terminal, a stored value terminal, a monetary access terminal, a PBX terminal, a long distance terminal, a personal computer, a laptop computer, a personal digital assistant, a public internet terminal, and an automated teller machine.

18. The method of claim 1, wherein presenting the biometric sample further comprises presenting at least one biometric sample selected from a group of biometric samples consisting of voice print, photograph, signature, fingerprint, hand geometry, retinal

WAVELYNX EX. 1003, Pg. 1583
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

image, and iris scan.

19. The method of claim 1, wherein automatically authenticating further comprises pre-selecting the desired probability of occurrence value.

20. The method of claim 19, wherein pre-selecting the desired probability of occurrence value further comprises pre-defining a desired probability of occurrence value for false acceptance of an impostor and false rejection of a valid user.

21. The method of claim 20, wherein pre-defining the desired probability of occurrence value further comprises pre-defining an instruction set directing the reader device to look to the stored table of probability of occurrence values for a false acceptance of an impostor and false rejection of a valid user threshold match score corresponding to the desired probability of occurrence value.

22. The method of claim 21, wherein automatically authenticating further comprises automatically selecting the false acceptance of an impostor and false rejection of a valid user threshold match score, such that for a desired false acceptance rate, a match value between the stored biometric information and the biometric sample is at least a pre-determined level, and for a desired false rejection rate, the match value is less than a pre-determined level.

23. The method of claim 1, wherein automatically authenticating further comprise automatically authenticating the user by an application associated with the reader device.

24. The method of claim 23, wherein automatically authenticating further comprises automatically authenticating the user by an application residing at least in part on the reader device.

25. The method of claim 23, wherein automatically authenticating further comprising automatically authenticating the user by an application residing at least in part on a terminal associated with the reader device.

26. The method of claim 1, wherein automatically authenticating further comprises automatically authenticating the user by an application associated with the smart card.

27. The method of claim 26, wherein automatically authenticating further comprises automatically authenticating the user by an application residing at least in part on the smart card.

28. A system for authenticating a smart card user at a reader device, comprising:

means for storing information fields for the user on the smart card relating to biometric information for the user and a table of pre-defined probability of occurrence values for user authentication;

means for presenting the smart card and a biometric sample for the user to the reader device;

means associated for automatically authenticating the user by the reader device based at least in part on a match level between the stored biometric information and the presented biometric sample according to a desired probability of occurrence value from the stored table.

29. The system of claim 28, wherein the means for storing the information fields further comprises an application on the smart card.

30. The system of claim 29, wherein the application on the smart card further comprises an application on a microprocessor of the smart card.

31. The system of claim 30, wherein the means for presenting the smart card and the biometric sample further comprises a reader device associated with a terminal.

32. The system of claim 31, wherein the means for presenting the smart card and the biometric sample further comprises an application associated with the reader device.

33. The system of claim 32, wherein the terminal further comprises at least one of an area access terminal, a computer network terminal, a computer access terminal, a stored value terminal, a monetary access terminal, a PBX terminal, a long distance terminal, a personal computer, a laptop computer, a personal digital assistant, a public internet terminal, and an automated teller machine.

34. The system of claim 28, wherein the means for automatically authenticating the user further comprises an application associated with the reader device.

35. The system of claim 34, wherein the reader device is associated with a terminal.

36. The system of claim 35, wherein the terminal further comprises at least one of an area access terminal, a computer network terminal, a computer access terminal, a stored value terminal, a monetary access terminal, a computer access terminal, a stored value terminal, a monetary access terminal, a PBX

WAVELYNX EX. 1003, Pg. 1584
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

terminal, a long distance terminal, a personal computer, a laptop computer, a personal digital assistant, a public internet terminal and an automated teller machine.

37. The system of claim 28, wherein the means for automatically authenticating further comprises an application associated with the smart card.

WAVELYNX EX. 1003, Pg. 1585
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

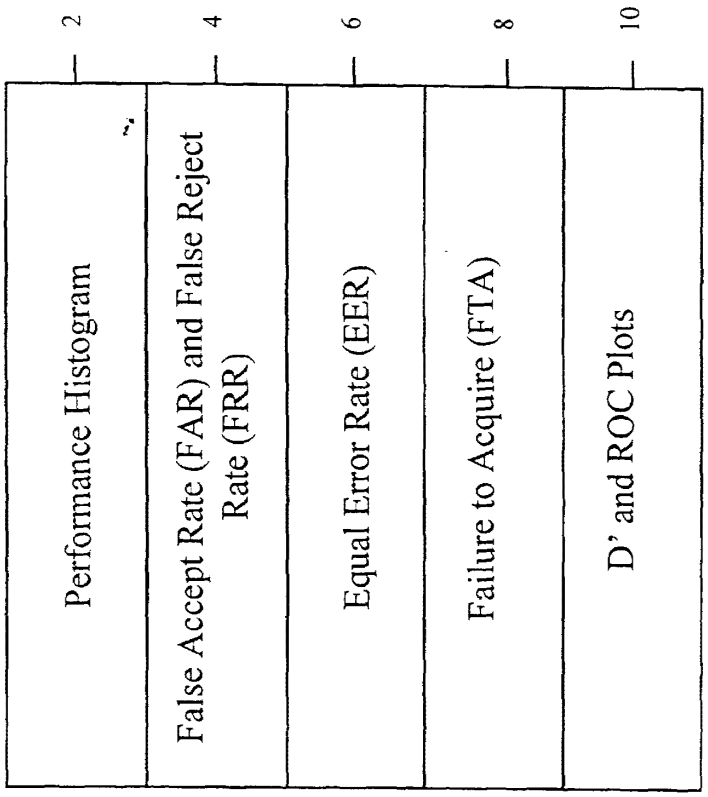


FIG. 1

WAVELYNX EX. 1003, Pg. 1586
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

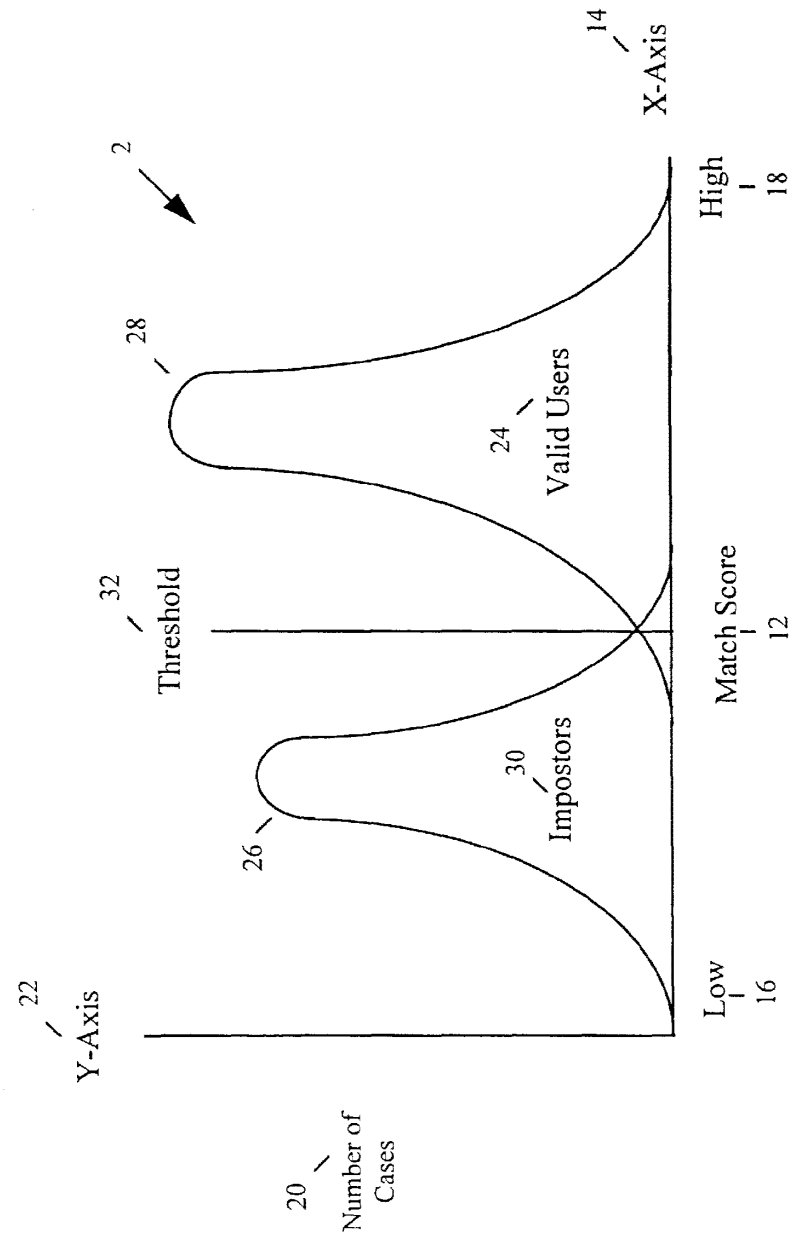


FIG. 2

WAVELYNX EX. 1003, Pg. 1587
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

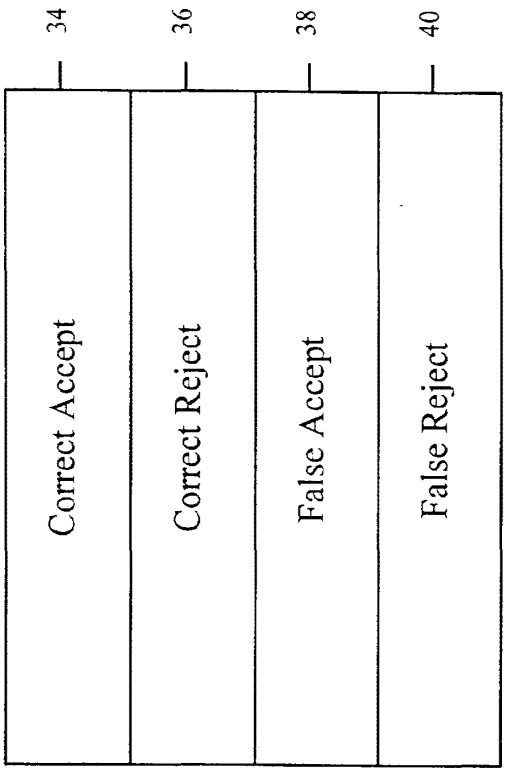


FIG. 3

WAVELYNX EX. 1003, Pg. 1588
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

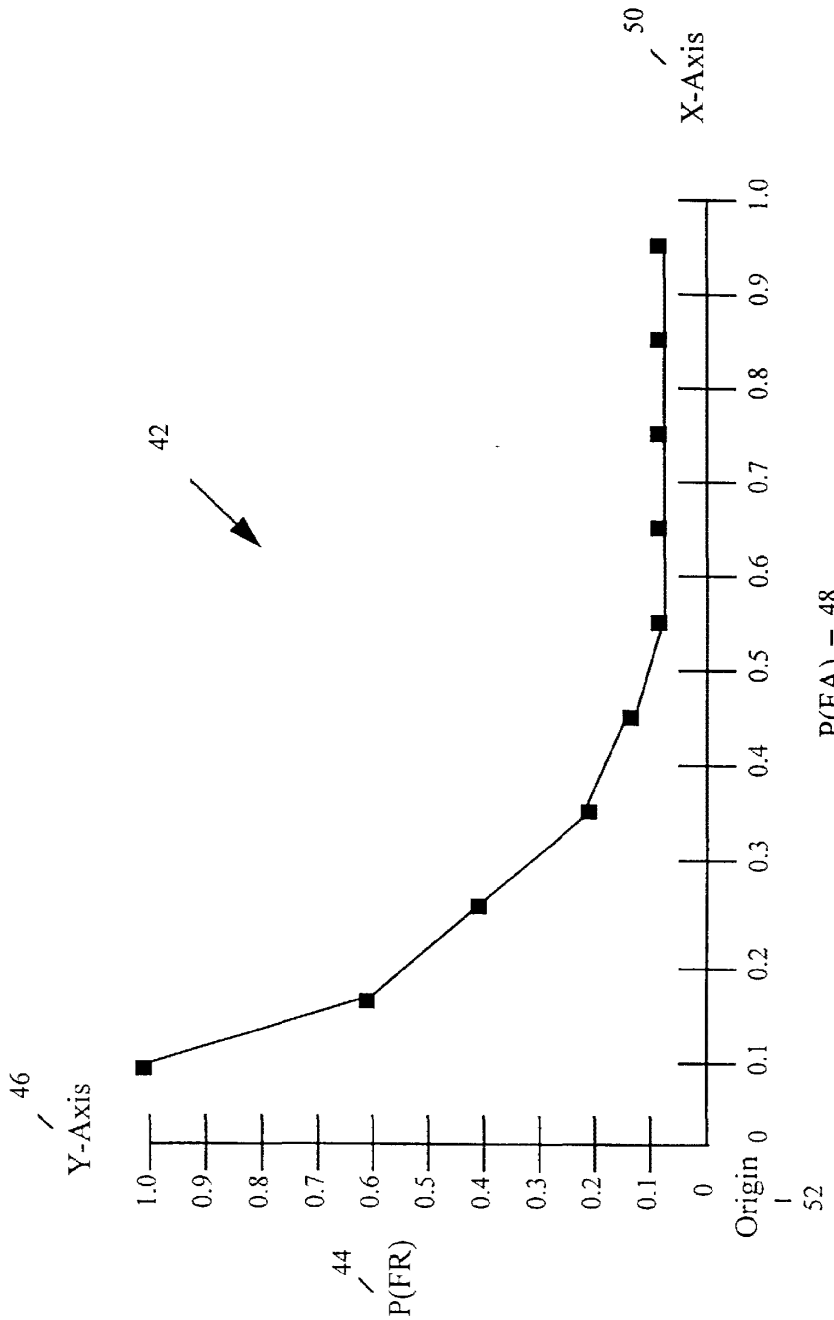


FIG. 4

WAVELYNX EX. 1003, Pg. 1589
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

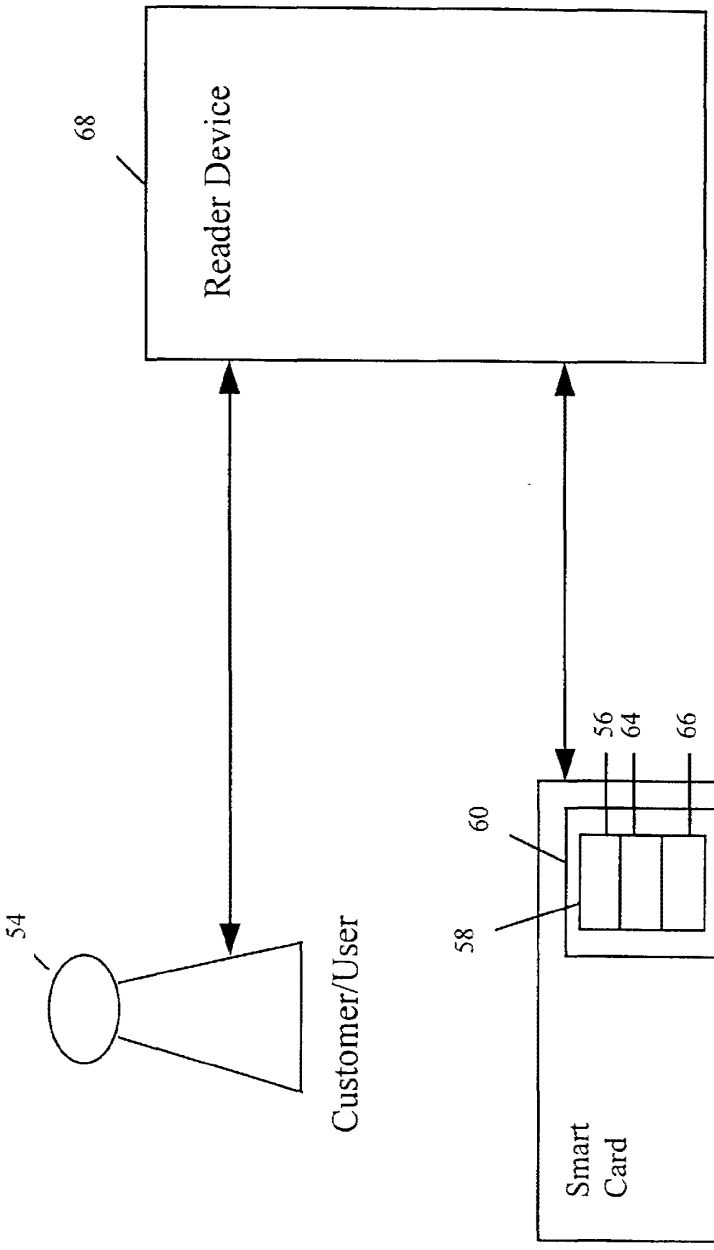


FIG. 5

WAVELYNX EX. 1003, Pg. 1590
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

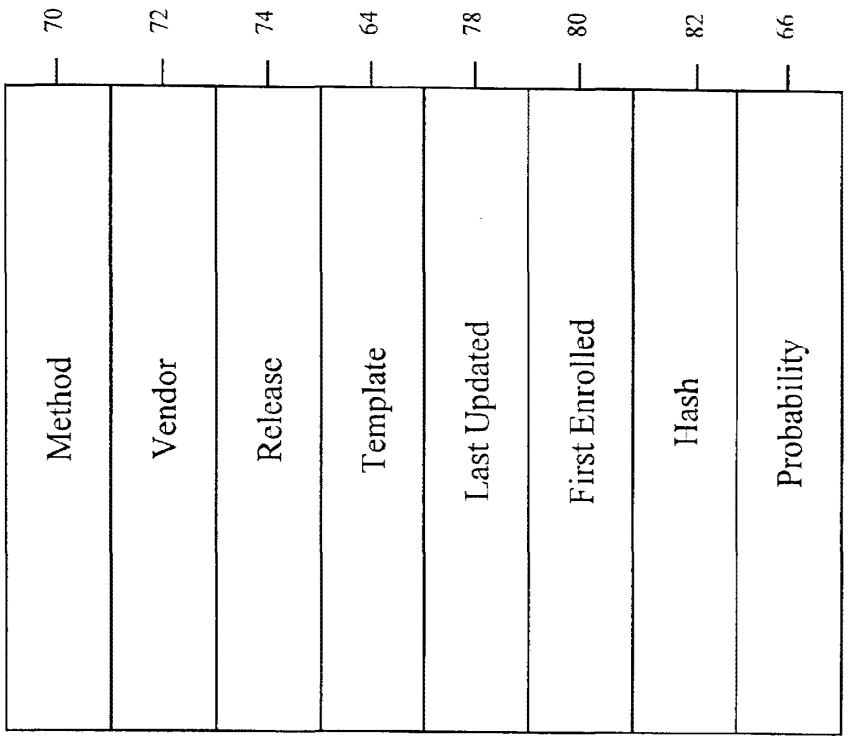


FIG 6.

WAVELYNX EX. 1003, Pg. 1591
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

66

PROBABILITY	FA	FR
1/100	200	700
1/1000	300	600
1/10,000	400	500
1/100,000	500	400

FIG. 7

WAVELYNX EX. 1003, Pg. 1592
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

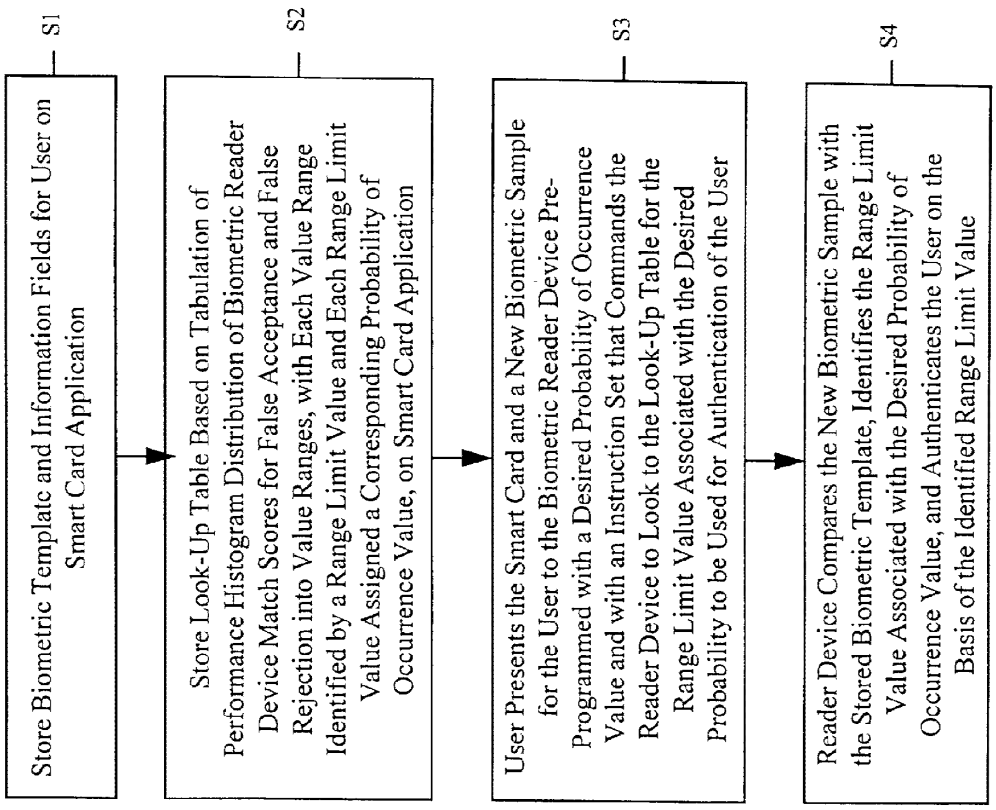


FIG. 8

WAVELYNX EX. 1003, Pg. 1593
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 20 1446

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP 0 612 035 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 24 August 1994 (1994-08-24)	1,18,19, 28	A61B5/117 G06K9/00
Y	* page 1, line 49 - page 2, line 7 * * page 5, line 35 - line 38 *	12-17	
X	GB 2 237 672 A (DE LA RUE SYSTEMS LTD) 8 May 1991 (1991-05-08) * page 2, line 8 - page 5, line 25 *	1-3,18, 28	
Y	* page 9, line 23 - page 10, line 8 *	4-9, 19-27, 29,30, 34-37	
Y	WO 91 07729 A (THE SECRETARY OF STATE FOR DEFENCE ET AL) 30 May 1991 (1991-05-30) * page 1, line 4 - line 8 * * page 6, line 33 - page 8, line 33 *	1,4-8, 19-25,28	
Y	US 5 111 512 A (JASON CHIA-SUN FAN ET AL) 5 May 1992 (1992-05-05)	1,28	TECHNICAL FIELDS SEARCHED (Int.Cl.6)
A	* column 2, line 58 - column 5, line 2 *	4-8, 18-22	A61B G06K
Y	GB 2 248 513 A (ENSIGMA LTD ET AL) 8 April 1992 (1992-04-08) * page 4, line 9 - line 20 *	1,28	
A	* page 8, line 32 - page 10, line 23 *	4-8, 18-22	
Y	WO 96 13800 A (THE NATIONAL REGISTRY INC ET AL) 9 May 1996 (1996-05-09) * page 7, line 24 - line 28 *	1,9, 12-17, 28,34-36	
A	* page 12, line 26 - page 14, line 33 *	31-33	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	20 August 1999	Geffen, N

CATEGORY OF CITED DOCUMENTS

X particularly relevant if taken alone
Y particularly relevant if combined with another document of the same category
A technological background
O : non-written disclosure
P intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1594
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 20 1446

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	"IDENTIFICATION AND VERIFICATION OF SIGNATURES" IBM TECHNICAL DISCLOSURE BULLETIN, vol. 39, no. 6, 1 June 1996 (1996-06-01), pages 93-97, XP000678532 ISSN: 0018-8689 * the whole document *	1,12,13, 26-30,37	
A	L. L. LEE ET AL: "RELIABLE ON-LINE HUMAN SIGNATURE VERIFICATION SYSTEM FOR POINT-OF-SALES APPLICATIONS" PROCEEDINGS OF THE IAPR INTERNATIONAL CONFERENCE ON PATTERN RECOGNITION, JERUSALEM, OCT. 9 - 13, 1994 CONFERENCE B: PATTERN RECOGNITION AND NEURAL NETWORKS, vol. 2, no. CONF. 12, 9 October 1994 (1994-10-09), pages 19-23, XP000509876 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERSISBN: 0-8186-6272-7 * the whole document *	1,4-37	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	20 August 1999	Geffen, N

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underly ng the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

WAVELYNX EX. 1003, Pg. 1595
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 20 1446

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

20-08-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0612035 A	24-08-1994	NONE	
GB 2237672 A	08-05-1991	NONE	
WO 9107729 A	30-05-1991	GB 2237917 A	15-05-1991
		US 5226091 A	06-07-1993
US 5111512 A	05-05-1992	CA 2066961 A,C	15-11-1992
		DE 69212890 D	26-09-1996
		DE 69212890 T	02-01-1997
		EP 0514082 A	19-11-1992
		JP 2699241 B	19-01-1998
		JP 6251130 A	09-09-1994
GB 2248513 A	08-04-1992	AU 665745 B	18-01-1996
		AU 8649691 A	28-04-1992
		WO 9206468 A	16-04-1992
		US 5526465 A	11-06-1996
WO 9613800 A	09-05-1996	US 5546471 A	13-08-1996
		AU 4230696 A	23-05-1996
		US 5920642 A	06-07-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

WAVELYNX EX. 1003, Pg. 1596
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 251 448 A1

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 158(3) EPC

(43) Date of publication:
23.10.2002 Bulletin 2002/43

(21) Application number: **00976467.1**

(22) Date of filing: **09.11.2000**

(51) Int Cl.[7]: **G06K 5/00**, G06K 19/00, G07F 7/10

(86) International application number:
PCT/RU00/00446

(87) International publication number:
WO 01/052174 (19.07.2001 Gazette 2001/29)

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **11.01.2000 RU 2000101180**

(71) Applicant: **TOO Mnogoprofilnoe Predpriyatie**
St.Petersburg, 198092 (RU)

(72) Inventors:
- **MINKIN, Viktor Albertovich**
  St.Petersburg, 196247 (RU)
- **GREKOVICH, Alexandr Anatolievich**
  St.Petersburg, 197349 (RU)
- **ROMANOVA, Ljudmila Pavlovna**
  St.Petersburg, 194021 (RU)
- **TATAURSCHIKOV, Sergei Sergeevich**
  St.Petersburg, 194223 (RU)
- **SHTAM, Alexandr Iliich**
  St.Petersburg, 197343 (RU)
- **ZONOV, Viktor Fedorovich**
  Leningradskaya obl., 188660 (RU)

(74) Representative: **Viering, Jentschura & Partner**
Steinsdorfstrasse 6
80538 München (DE)

(54) **METHOD, DEVICE AND SYSTEM FOR BIOMETRIC IDENTIFICATION**

(57) For the purpose of user biometric identification, at least one optical image of the selected user biometric parameter (BP), for example, its fingerprint, recorded on a suitable carrier - biometric key (20). The main operations of the identification method is simultaneous or alternating matching of the selected biometric parameter with the inlet optical surface of the readout sensor (57); readout of the specified parameter and its image by the readout sensor with generation of electronic codes of the readout parameter and readout image in the format providing a possibility of their comparison; comparison of the above-mentioned codes and output of the result of identification on the basis of the results of the given comparison. In its preferable version, the method also provides a stage of for the biometric key manufacture and the formation of database (38) of verified electronic codes of biometric parameters of the users to be subject to identification. User identification system (1) contains a subsystem (10) for the manufacture of biometric keys (20); a subsystem (30) for generation and storage of database (38) of the verified electronic codes of each specified biometric parameter of every user and at least one user identification device (42). This device (42) contains a readout unit (50) containing at least one readout sensor (57) equipped by a multi-element photo-detector (58); a lighter (52); a holder (54) for installation and fixation of any biometric key (20) and a processor unit (60).

EP 1 251 448 A1

Printed by Jouve, 75001 PARIS (FR)

WAVELYNX EX. 1003, Pg. 1597
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Description

Technical Field

[0001] The invention relates to biometric identification with optical reading of biometric information and can be used in any areas where it is needed to carry out user identification including security and access systems, various transactions including financial transaction with the use of personalised credit cards, passport systems for population, manufacture and use of various personalised documents such as driver's licenses, etc. Then to simplify understanding of the invention essence, it will be described mainly with the application to the use as a biometric parameter of one or several fingerprints. However the invention also covers the use of any other biometric parameters being suitable for the identification purposes, for example, retina images or user signatures.

Prior Art

[0002] The user identification methods are known that use information not connected with a biometric parameter containing, for example, a personalized identification number (PIN) recorded directly on a plastic card or in the memory of a contact or contact-free chip located on the same plastic card or a special carrier. Information recorded on such card can represent a non-repeatable number or support a ciphered exchange dialogue between the information carried and the reading system (US 6068184, US 5991749). These methods and systems are easy and reliable in operation but are not protected against unauthorised use after loss of the carrier, which can be used by any person.

[0003] At the present time, a whole number of user identification systems are known, which use biometric dactyloscopic information. The principle of operation of most similar systems is based on optical reading of a biometric parameter of the user being identified by means of the corresponding reading device, conversion of the readout information into a digital electronic code and search in the database for an electronic code matching, in essence, this electronic code. If such matching takes place, then a signal on a positive result of the user identification will be issued. Similar systems and identification methods implemented therein as well as devices being used in the given systems are described, for example, in US 4933976, US 4932776, US 4785171, US 4690554, US 4582985.

[0004] The known systems implementing this principle contain various biometric parameter reading devices differing, in particular, by the type of photo-receiver being used and by the lighter design. So in WO 98/27509, a user identification device is described, which allows to enter a live finger image with a high image quality and which contains a lighter illuminating the user finger and the sensor with the inlet fibre-optic surface, onto which the user finger is put.

[0005] Light scatters in the finger and passes through the skin in places (lines) pressed against the inlet surface, with minimal losses; at places not pressed against the surface (in hollows), the light losses are considerably high. Because of that, an optical image is being created and an electronic fingerprint image based thereon, which is then converted into an electronic code for the image being read out. The lighter design of this device is optimised with the account of light scattering peculiarities in a real ("live") finger, which restricts the use of the given device and the method, which it implements, by the identification by real fingerprint at its comparison with the electronic codes being stored in the database.

[0006] Instead of storing user biometric parameter codes in the database, they can be recorded on biometric keys being plastic cards to be issued to users and read out from these keys in order to be compared with a signal being obtained as a result of the corresponding conversion of the read-out biometric parameter, as it has been described, for example, in US 4993068, US 5598474 and US 5623552. The identification signal is issued in case of mutual correspondence of the information written on the card and obtained at the biometric parameter readout.

[0007] In particular, a possibility is known to write information, including that on a plastic card, in the form of a two-dimensional bar-code (US 5548110, US 6062481). However recording of dactyloscopic information or a fingerprint code may contain approximately 1 Kbyte, and a two-dimensional bar-code of such size will occupy almost half of the plastic card. Consequently, recording of information about two fingers of the user on one plastic card is practically impossible, since besides dactyloscopic information, PC should provide space for recording the user demographic data. In addition, two-dimensional bar-code readout devices are sufficiently sophisticated and expensive, which also impedes the use of this bar-code for recording of dactyloscopic information on plastic cards in mass projects, in spite of a low cost of the card itself.

[0008] A common shortcoming of known identification systems with the use of a contact-free chip plastic card is also a high level of expenses, which is especially sensible at the implementation of such mass personalised projects as issuance of national passports, driver's licenses and other documents. The cost of such projects will be determined mainly by the cost of chip plastic cards. For example, the issue of passports for 100 million people based on a chip plastic card costing approximately USD 15 will require USD 1.5 billion.

[0009] The use of contact chip cards for passport project is impossible, as, in spite of a considerably lesser cost (USD.3-5 on average), the reliability of the contact chip operation is not sufficient, as they can easily be subject to destruction.

[0010] In connection with the above-listed drawbacks, these devices and systems have not yet reached mass

WAVELYNX EX. 1003, Pg. 1598
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

application.

[0011] A system is also known (described in US 4983036), where information written on a plastic card, which is used as a biometric key, is the optic image of a fingerprint. In the identification process, this image is to be compared with the optical image of the real fingerprint by means of autocorrelation of the image of the optically projected fingerprint-reflected light in respect of the fingerprint on the card. A similar comparison method is very laborious and unreliable.

Summary of the Invention

[0012] The main task, which is the target of this invention, is to ensure a simple, convenient and reliable user biometric identification with the use of at least one optical biometric parameter image being formed on the biometric key.

[0013] A further problem is to provide a simple, convenient and reliable user biometric identification with the use of at least one optical biometric parameter image being formed on the biometric key, functioning without the necessity of calling of the verified electronic code database.

[0014] The next problem is to secure a simple, convenient and reliable user biometric identification with the joint use of at least one optical biometric parameter image being formed on the biometric key and the information being obtained at the direct reading of the similar biometric parameter by means of an optical readout device or a readout unit.

[0015] Another problem is to provide an opportunity to carry out user biometric identification with the use of two protection levels based on verified dactyloscopic information and with the use of one and the same optical readout device or a readout unit for reading of at least one optical image from the biometric key and the similar "real" biometric parameter.

[0016] This invention providing the solution of the above listed and other problems, which will be clear from the detailed description of the inventions given hereinafter, is based on the experimental establishment of a possibility of reading of optical images of some biometric parameters, first of all, of fingerprints, from the surface of a plastic carrier manufactured from a material with the integral absorption of optical radiation in certain spectrum regions being close to finger absorption. Accordingly, this invention based on the use of optical images of biometric parameters written on a certain plastic carrier (hereinafter referred to as the "biometric key"), represents, in its first aspect, a user identification method including preferably the following operations:

(f) matching of the image of the selected biometric parameter for an individual user, for example, his/her fingerprint, with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval; at that the above-mentioned image has been formed on the biometric key of the given user in the area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval;

(g) readout of the above-mentioned image by the readout sensor with generation of the electronic code of the image;

(j) matching of the selected biometric parameter with the inlet optical surface of the reading sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;

(k) readout of the above-mentioned biometric parameter with generation of the electronic code of the readout parameter in the format providing a possibility of comparison of this electronic code with the above-mentioned electronic code of the readout image,

(m) comparison of the electronic code of the readout biometric parameter and the electronic code of the readout image; and

(n) output of the user identification result based on the results of comparison of electronic codes of the biometric parameter and the readout image.

[0017] In one of its preferable implementation options, the method concerning this invention also provides a stage for the biometric key manufacture and the formation of a database of verified electronic codes of biometric parameters of the users to be subject to identification, this stage including the following operations:

(a) selection of the biometric parameter for an individual user, for example, his/her fingerprint;

(b) generation of the optical image of the selected user biometric parameters from a variety of users;

c) recording of the generated image with the scaling being equal or close to 1 on a blank for the biometric key of the given user in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval;

(d) generation of at least one verified electronic code of the selected biometric parameter and its saving for permanent storage in the selected format in the form of a set of digital signals unambiguously corresponding to the specified biometric parameter;

(e) repeated execution of operations (b), (c) and (d) for the remaining users out of the variety of users with obtaining of one biometric key for each user and with generation of the database of verified electronic codes of selected biometric parameters;

[0018] In order to enhance the identification reliability,

WAVELYNX EX. 1003, Pg. 1599
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

the method under this invention can also include additionally the following operations:

(j) combination of the selected biometric parameter of the user being identified with the above-mentioned inlet optical surface of the reading sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;
(k) readout of the specified biometric parameter with generation of its electronic code providing a possibility of comparison of the electronic code of the readout biometric parameter with the verified electronic codes;
(l) search for a verified electronic code coinciding, in essence, with the electronic code of the readout biometric parameter,

with operation (i) additionally including the results of operation (l).

[0019] In this implementation version, the identification method at the stage of biometric key manufacture preferably includes the operation of

(o) generation of all verified electronic code of the selected biometric parameter and its saving for permanent storage for all users out of the variety of users in the form of a set of digital signals unambiguously corresponding to the specified biometric parameter, with generation of the database of verified electronic codes of selected biometric parameters in the format providing a possibility of comparison of the electronic code of the readout biometric parameter with the verified electronic codes;

[0020] in addition, operation (m) consists of comparison of the electronic codes of the readout biometric parameter and the readout image with verified electronic codes, and a decision on the positive identification result shall be taken at the detection of a verified electronic code, which, in essence, coincides with the electronic code of the readout biometric parameter and/or readout image.

[0021] Examples of materials especially suitable for manufacture of the biometric key are polyvinylchloride (PVC) or polyester (PET), which are conventionally used for the plastic card manufacture. At that, the best results of the readout of optical biometric parameter images are reached at the uniform illumination of the carrier in transmitted light within the selected spectral interval, which preferably lies in the near infrared region (0.75 - 1.0 μm). In this case, the preferable thickness of the optical image carrier equals to about 0.8 mm, i.e. coincides with the standard thickness of plastic cards. It is evident that the reverse side of the plastic card (opposite to the side, on which the biometric parameter image, for example, fingerprint image, is applied) shall not contain images being non-transparent in the selected region of the spectral interval, as the availability of such images may lead to the appearance of significant disturbances on the readout biometric parameter image.

[0022] The authors of the invention have experimentally established that any colour and grey-scale black-and-white printing of standard printers and DataCard (Image Card Express Photo ID Printer, DataCard 9000) and Fargo (Pro-L, Quatro) plastic card printing systems is transparent in the selected spectral range whereas printing from a black tape is practically non-transparent in the specified spectral range.

[0023] The next condition providing a high readout quality is scaling of the biometric parameter image at its generation on the biometric key. There is the only difference in the resolution of readout facilities and means generating the image. For example, normal thermal printing facilities for plastic cards have the resolution not higher than 300 dpi whereas the image readout facilities can have the resolution up to 3000 dpi. Analysing large dactyloscopic image archives, the authors have established that the number of visible dactyloscopic peculiarities suitable for identification increases as the resolution of a dactyloscopic scanner grows. As a consequence of this dependence, it appears that, for example, at printing of a fingerprint image or its part enlarged proportionally to the reduction in the area with constant resolution, an approximately equal number of critical points both on the whole fingerprint and on its part. Consequently, the location of the enlarged image of the central part of the fingerprint on the plastic card is an additional measure allowing to avoid errors during the identification, as at every placing of the user finger, the probability of presence of the central fingerprint part is considerably higher than that of its edge parts.

[0024] At least two images of the corresponding biometric parameters can be generated on one biometric key preferably made in the form of a plastic card. An opportunity to place several fingerprint images on one plastic card significantly increases the probability of proper identification; the central-symmetrical location of fingerprints on the plastic card allows not to use moving mechanical parts in the readout unit of the identification device.

[0025] According to the second aspect of this invention, in order to execute all above-listed operations of the proposed method, it is provided to create a user identification system containing the following:

a means for recording of at least one image of one biometric parameter of an individual user out of the variety of users, for example, his/her fingerprints, on a biometric key blank, in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval;
a subsystem for generation and storage of the database of verified electronic codes for each speci-

WAVELYNX EX. 1003, Pg. 1600
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

fied biometric parameter of every user out of the variety of users; and
at least one user identification device.

[0026] In accordance with the next aspect of this invention, it is also provided to create a new user identification device, which contains the following:

a readout unit containing at least one readout sensor equipped by a multi-element photo-detector being sensitive in the selected spectral interval of the optical range; in addition, the readout unit is made with a possibility of reading the image from a biometric key out of the variety of biometric keys, each of which is intended for identification of user out of the variety of users and contains an image area made from a material being semi-transparent in the selected spectral interval of the optical range, in which an image of the biometric parameter of the specified user has been generated with the selected scaling;
a lighter providing uniform illumination of the readout sensor by radiation in the selected spectral interval of the optical range;
a holder for installation and fixation of any biometric key out of specified variety of keys with bringing of the image generated thereon into contact with the inlet sensitive surface of the readout sensor; and
a processor unit connected to the readout unit outlet and equipped by means for the generation of an electronic code of the readout image and by means for comparison of the electronic code of the readout image with other electronic codes with generation of the first signal in case of detection of coincidence of the electronic code of the readout image with any other electronic code and with generation of the second signal, if no above-mentioned coincidence has been detected.

[0027] Besides those mentioned above, one more preferable condition providing high quality readout is the use of a readout sensor with the inlet fibre-optic surface, against which the image being read out must be tightly pressed. At the performance of this and other conditions listed, a possibility of using similar or even one and the same optical readout sensor for reading a real biometric parameter (a fingerprint, i.e. a relief object) and its flat carrier from the plastic carrier.

[0028] The use of one sensor for reading both a live finger image and a visible image from the card allows to simplify the identification device design and operations to be executed by the user at the implementation of the identification method under this invention. In addition, the system operation reliability gets considerably enhanced, as unlike a chip PC a fingerprint being stored in the form of a real visible image on the biometric key made in the form of a plastic card has a good noise immunity and does not sensitive to electric and magnetic fields. Another advantage of this device is an additional possibility of future modernisation and the compatibility meaning that the software identification algorithms are being constantly improved, with the main modifications concerning conversion of the image into a compressed code. In a chip, only a compressed code is stored, which will not allow or impede a future use of any new software. The information storage in the form of an optical image of the biometric parameter will allow to use all future software improvements without any considerable expenses, this being simultaneously for reading of both the biometric parameter itself and its image on the biometric key.

[0029] The above-listed advantages make it impossible to broadly use the proposed invention, both for local systems and for global projects, for example, national passport system, authorisation of access to Internet or additional protection of credit cards.

[0030] The remaining distinctive signs and advantages of this invention will become clear from the detailed description of preferable versions of its implementation given below as well as from the invention formula being enclosed herewith.

Brief description of drawings

[0031]

Fig. 1 shows one of the preferable versions of embodiment of the user identification system under this invention in the form of a flow-chart;
Fig. 2 shows the front side of a plastic card;
Fig. 3A contains a user identification device in the form of an arrangement with the biometric key being introduced therein;
Fig. 3B shows the same device with a user finger being placed into it;
Fig. 4 shows a set of operations to be executed at the first stage of one of the preferable versions of implementation of the method under this invention;
Fig. 5A, 5B show a non-processed image and a processed image of one and the same fingerprint respectively;
Fig. 6, 7 and 8 show sets of operations to be executed at the second stage of two preferable versions of implementation of the method under this invention.

Description of preferable implementation of the invention

[0032] The system version shown in Fig. 1 and designated on the whole as 1 is intended mainly for operation with biometric keys in the form of plastic cards with the standard parameters in accordance with ISO 7810-85 and sizes in accordance with CR80. However it can also be used for manufacture and use of many other versions of biometric keys. As shown in Fig. 1, sys-

WAVELYNX EX. 1003, Pg. 1601
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

tem 1 consists of several interconnected parts, or subsystems, the main from which are subsystem 10 for manufacture of biometric keys 20, subsystem 30 for generation and storage of the verified electronic code database and subsystem 40 for identification.

[0033] Subsystem 10 for the manufacture of biometric keys includes a set of necessary technical means or devices to execute various operations provided by the key manufacture technology being used in the system. It is evident that the composition of this set and the form of embodiment of its components considerably depend upon a specific version of the identification key being used. However an obligatory part of any version of system 10 are means for recording the optical image of the selected biometric parameter on biometric key 20. These means of recording preferably include device 12 for generation of an image of the selected biometric parameter with the conversion of this image into its electronic copy, i.e. into a set of electrical (or other) signals unambiguously corresponding to the image being generated. Device 12 can operate in any wavelength range and/or use any suitable image generation and conversion means provided the quality of the electronic copy being obtained is sufficient for the subsequent creation of an optical image on the biometric key being suitable for the performance of the user identification function. As device 12, for example, any scanner or a device for reading biometric parameters, for example, a dactyloscopic scanner, can be used for obtaining of a fingerprint image and/or a television camera for obtaining of user retina or face images.

[0034] Another, not obligatory but preferable, component of subsystem 10 is device 14 for electronic copy processing. The type of processing being performed by this device will be explained later at the description of the identification method under this invention. A preferable version of implementation of device 14 is a personal computer equipped by the corresponding software program for processing images and by necessary peripheral devices, including keyboard 15, display 16 as well as an interface (not shown) for reading electronic copies being supplied from the outlet of device 12 for image generation.

[0035] The third component of the means of recording is device 18 for application of an optical image on biometric keys 20. Preferably, device 18 is a printer for personalisation of plastic cards connected to the outlet of device 14 and customised for printing images in case f obtaining of processed or non-processed electronic copy from device 14.

[0036] Fig. 2 shows a conventional image of the front side of the biometric key pattern in the form of a personalised plastic card with standard parameters in accordance with ISO 7810-85 and sizes in accordance with CR80 (85 mm x 54 mm x 0.8 mm). As shown in Fig. 2, two areas 22 of image are provided for printing the image on biometric key 20, which are made from a material being semi-transparent in the selected spectral interval of the optical range (for example, 0.75 - 1.0 μm, i.e. in the near IR-region). If the biometric key is a plastic card, then the whole card can be made from this material. In particular, suitable materials for area 22 and the biometric key on the whole are polyvinylchloride and polyester.

[0037] It can be seen from Fig. 2 that biometric key 20 may, beside a biometric parameter image or several similar images (for example, fingerprints of two or more different fingers of the user), also contain any other necessary information in the wording, digital, symbolic, graphical. Electronic, magnetic or any other suitable form.

[0038] An additional information can be written on the biometric key at the same time with recording of the biometric parameter image, with the use of one and the same device 18 for the application of images, or at any other suitable stage of the biometric key manufacture, with the use of any means being suitable for this purpose. As these means are well-known to specialists, there is no need of describing them. The use of thin transparent laminating coatings allows to increase the plastic card service life and does not impede the reading of biometric images from a plastic cards in the reflected and transmitted light. A card can be created with an increased protection and secrecy, as it has been described, for example, in US 4999065. However the availability of an image of the user biometric parameter directly on a plastic card provides its protection better than any other complicated systems, as it makes it practically impossible to use cards by any other person rather than the user. Coded information can be additionally recorded into biometric key 20, for example, in the form of an n-dimensional bar-code, with the coded information recorded area being selected close to the image size. The coded information may contain, for example, data on the user biometric parameter. In this case, the optical image and the coded information will preferably be recorded by means of various printing means, for example, various paints being non-transparent and/or reflecting radiation in various spectral intervals of the optical range. It is also desirable that the image and the coded information should be placed in a single readout area, which dimensions are determined by dimensions of the photosensitive surface of the readout sensor but are separated spatially. In this case, the image is preferably located in the centre of the readout area and the coded information is located in the edge zone of this area.

[0039] The main component of subsystem 30 for generation and storage of the verified electronic code database is processor 32 equipped by the corresponding peripheral devices 34 and connected with the outlet of processing device 14 for the reception of processed electronic copies of optical images being generated by this device. In the preferable version of implementation, subsystem 30 is a personal computer. As it will be described in detail later, this subsystem is designed for the conversion of electronic copies coming from device 14 into verified electronic codes of the corresponding user

WAVELYNX EX. 1003, Pg. 1602
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

biometric parameter (or biometric parameters) as well as for generation and storage of database 38 of such codes. In the alternative version of implementation of subsystems 10 and 30 (not shown), processing device 14 is a part of subsystem 30, which one outlet in this case shall be connected with device 18 for application of optical image on biometric key 20. It is possible to implement subsystem 30 and device 14 for the electronic copy processing on one personal computer.

[0040] Identification subsystem 40 in its preferable version is an identification device 42 connected to database 44 of subsystem 30 data with a possibility of data exchange. One of the preferable versions of implementation of device 42 is given in Fig. 3. In this version, device 42 contains a readout unit 50 and a processor unit 60 connected to the readout unit outlet. Readout unit 50 in the given version consists of a lighter 52, a holder 54 of biometric key 20 in the form of a plastic card and a readout sensor 57 with a multi-element photo-detector 58 (matrix or linear) being sensitive in the selected spectral interval of the optical range.

[0041] At the use of the biometric key in the form of a plastic card and at the selected spectral interval in the near IR-region, the preferable version of photo-detector 58 is a matrix detector with the size of photo-detecting surface being not less than 8 x 12 mm, with the number of photo-detecting elements being not les than 200 x 300, with a fibre-optic washer 59 generating the inlet surface of sensor 57. A specific version of the sensor can be the DactoChip DC-21 model with the size of photo-detecting surface being equal to 10 (H) x 15 (V) mm and with the number of photo-detecting elements of 512 (H) x 576 (H), with the fibre-optic washer of the brand ИАШО 200370002 TY with the diameter of one optical fibre being equal to 6 μm. At the use of photo-detector 58 in the form of a ruler, the device can be equipped by a scanning mechanism providing reciprocal photo-detector movement in the plane being parallel to the plane of fibre-optical washer 59. Alternatively, scanning can be carried out by moving the biometric parameter in respect to the ruler of photo-detector 58.

[0042] Lighter 52 is preferably made of the impulse type and contains not less than one light-emitting diode (LED), for example two LEDs of the brand ИРС-1-800/90 emitting light in the selected spectral interval (λ = 800 nm, $\angle$ = 90°).

[0043] It was assumed earlier that in order to obtain a uniform fingerprint image in the light transmitting through the finger, it shall be illuminated non-uniformly directing more light into the volumetric part of the figure, as it is known that the light scattering in any medium, including finger, is proportional to the light transmission path.

[0044] The authors of the invention have experimentally proved that such diffuse scattering really occurs at the local illumination of the finger by a narrow-directed light, however this fact with application to this invention is not significant, as the narrow-directed illumination is unsuitable for raying of thin (as compared with a finger) plastic cards, as it creates a high light non-uniformity. At the same time, the authors have experimentally established that at the initial uniform diffuse illumination of the sensor surface, the same uniform illumination (raying) occurs for both the plastic card and the finger at the use of a lighter operating in the near IR-region of the spectrum.

[0045] Holder 54 shall tightly press the plastic card against the inlet surface 59 of sensor 57 and at the same time not admit any surface damage of plastic card 20 at its mechanical movement between the surfaces of holder 54 and sensor 57. In order to meet this requirement, holder 54 is preferably made from a metal (for example, aluminium), on which internal (contacting with the plastic card) side 55 a layer 56 of a fluffy material (optical suede) is glued. Such design provide an easy and high-precision placing of the plastic card over sensor 57 without the use of moving mechanical parts in the design of readout unit 50.

[0046] A distinctive peculiarity of the readout unit 50 in the given version of the device is the fact that is provided a possibility of bringing into contact with the inlet surface 59 of sensor 57 of not only the biometric key 20 but also directly any finger of the user being identified, as it is schematically shown in Fig. 3B. So holder 54 combines two functions: it fixes both the plastic card, and the user finger. To this end, holder 54 in the centre has a hollow enabling the user to fix a finger conveniently on the inlet surface of the sensor. Normally the finger holder is installed tightly pressed against the dactyloscopic sensor (sensor 57). However the fixation of the bottom plane of the holder, proposed by the authors and shown in Fig. 3, at the height of the plastic card in respect of the inlet surface of the sensor also allows to provide a good contact between the user finger and the inlet surface of the sensor. It is evident that in the given holder the illumination of the finger being placed into it is provided from the side being opposite to the area of contact between the finger and photo-detector 58 and can be carried out from the top or from the sides.

[0047] Processor unit 60 is preferably made on the basis of a suitable personal computer of the PII-400 level with the corresponding peripheral devices (not shown). This computer is connected to the outlet of the readout unit 50, for example, by means of the corresponding cable connected to the parallel port of the computer. The processor unit 60 shall be equipped by means for generation of the electronic code of the readout image and the readout biometric parameter as well as by means for comparison of the electronic code of the readout image with the electronic code of the readout biometric parameter or verified electronic codes. These means are preferably software programs, for example, made on the basis of a standard dactyloscopic identification program; however any of then can also be implemented in the form of a separate specialised electronic module being a part of a computer or made sep-

WAVELYNX EX. 1003, Pg. 1603
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

arately from it.

[0048] In the case when coded data are additionally applied on the biometric key, for example in the form of an n-dimensional bar-code, readout unit 50 and processor unit 60 shall be made with a possibility of reading of the specified data and it decoding respectively. Meeting if this condition is facilitated at placing of the readout image and the coded information in a single readout area, due to which a single readout sensor 57 can read out both the image and the coded information.

[0049] Then the main stages of the identification method under this invention will be described.

[0050] The first stage 100, when the manufacture of biometric keys and preferably databases takes place, is performed with the use of subsystems 10 and 30 shown in Fig. 1. As shown in Fig. 4, the implementation of this stage begins from operation 102 for the biometric parameter selection of a biometric parameter (or parameters) for system 1. The second operation 104 consists of the input of the selected user biometric parameter included into the variety of users by system 1, in the field of vision of the image generation device 12 of subsystem 10. With application to the considered version of the method under this invention, the selected biometric parameter is a print of a certain user finger.

[0051] The next operation 106 for generation of the optical image of the selected biometric parameter of the given user, i.e. obtaining of optical information unambiguously corresponding to the given biometric parameter, is carried out with the use of the corresponding device 12 of subsystem 10 (see Fig. 1), for example, a readout unit (similar to unit 50 shown in Fig. 3b), which also performs the subsequent operation 108 for conversion of the optical information into electric information, with obtaining of an electronic copy of the biometric parameter, i.e. the corresponding set of electric signals unambiguously matching the specific biometric parameter.

[0052] The next operation 110 is coding, i.e. conversion of the electronic copy into the digital code of the selected biometric parameter. As it is shown in Fig. 1, this operation is executed in device 14 for electronic copy processing connected to the outlet of device 12.

[0053] It is expedient to use device 14 also for execution of operation 112 - electronic copy processing with isolation of information from'it necessary and sufficient for the biometric parameter identification. This operation preferably includes binarisation of the electronic analogue of the grey-scale fingerprint being generated by device 12 (see Fig. 5A) with obtaining of the processed analogue, so-called "skeleton" (see Fig. 5B) of a fingerprint with constant line thickness reflecting only those image features, which are taken into account at identification. The image processing monitoring can be carried out, for example, by means of a display 16 being a part of subsystem 10. The electronic copy of the selected biometric parameter being processed is fed to a printer or any other suitable device 18 for application of an optical image in order to execute operation 114 for recording of the processed optical image at the biometric key blank, with obtaining of biometric key 20. As it has been mentioned, this record is made in the image area made from a material (for example, polyvinylchloride) being semi-transparent in the selected spectral interval of the optical range. The recording is performed with the scaling being equal or close to 1, i.e. the processed fingerprint image being recorded (see Fig. 5B) by its dimensions equal or close to the real fingerprint, and, more precisely, to those parameters, which are taken into account at identification, namely: reflects the papillary line pattern. In order to carry out the recording, paints or other printing means are used, which are non-transparent or reflect radiation in the specified spectral interval, for example, a black tape of the Pro-L printer manufactured by Fargo.

[0054] Operation 114 for the processed image recording can also provide recording of any user data or any other necessary information on a blank of the biometric key 20, for example, that given in Fig. 2. This information can be entered into subsystem 10 by means of peripheral devices, for example, keyboard 15 or any external systems not shown in Fig. 1. In the alternative version, any other information (which application on the biometric key is not obligatory for the implementation of the method being described) can be recorded on the biometric key both before and after execution of operation 114.

[0055] After that, with the use of subsystem 40, procedure 201 is performed for the user identification according to the biometric key 20 and the selected fingerprint (performance of the given identification version will be described later, with reference to Fig. 6). In case of an identification failure, the key is rejected and the operations described shall be repeated in order to manufacture a valid key.

[0056] In case of confirmation of identification, the biometric key is recognised valid and can be issued to the user (operation 116). In this case, the digital information being used for recording of the optical image on the biometric key will also enter into subsystem 30 for generation and storage of the verified electronic code database. Here in processor 32, its processing will be completed, i.e. operation 118 for generation of the verified (i.e. unambiguously matching) electronic code of the selected biometric parameter, which enters for storage into database 38 (operation 120).

[0057] All operations described above are performed for all persons included into the variety of users by the identification system under this invention.

[0058] For the simplicity of understanding, the first stage of implementation of the given method was described in the simplest version. It is evident that in case of identification by several biometric parameters, operations 102-120 shall be repeated for each of the parameters. In order to enhance system operation reliability, several optical images can be generated for each selected biometric parameter at the execution of operation

WAVELYNX EX. 1003, Pg. 1604
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

106, out of which, upon results of the reference identification, the final selection of one image being the best or generalised to be applied on the biometric key shall be carried out. In this case, verified electronic codes of all generated optical images of one biometric parameter cab be formed and entered into database 38.

[0059] The enhancement of the identification system reliability can also be reached by the manufacture of all or at least a part of biometric keys in several copies.

[0060] The with the reference to Fig. 1, 3 and 6, one of the preferable versions of implementation of the second stage of the proposed method will be considered, namely, the conduction of user identification by biometric key. In order to implement this version, it required to provide a possibility of access from means 68 for electronic code comparison of the processor unit 60 of the identification device 42 to database 38 of system 1, as shown in Fig. 1. Alternatively, the whole database 38 or its corresponding fragment can be transferred into the identification device 40, which in that case can operate fully independently. This version can be expedient, for example, in cases when the manufacture and use of biometric keys is carried out in different organisations or if a variety of independently functioning identification devices is used installed at a considerable distance from the place of location of subsystem 30 for generation and storage of the verified electronic code database.

[0061] It can be seen from Fig. 6 that in this version the identification stage 201 includes procedure 210 for obtaining of an electronic code of the image. For its execution, the user shall enter his/her biometric key into holder 54 of the readout unit 50 of the identification device 42, i.e. perform operation 212 of matching of the biometric parameter image on the biometric key 20 with the inlet optical surface of the readout sensor 57. The readout unit consecutively executes operations 214, 216 for reading out of the specified image and generation of an electronic code of the image. At the execution of operation 216, the same electronic code format is used as at generation of the verified electronic codes (during operation 118) or any other format permitting a possibility of comparison of the electronic code of the image with the verified electronic codes. Procedure 210 is terminated by operation 218 for recording of the electronic code of the image.

[0062] Then operation 230 for the search in database of a verified electronic code, which, in essence (i.e. with the accuracy up to the established matching threshold), coincides with the electronic code of the readout image. The reliability of such search is very high, in the first place, because the image recorded on the biometric key is optimised for the search purposes by means of exclusion of all excessive and interfering information (as it was described earlier) and, in the second place, due to the fact that the key manufacture technology provides a high image stability in time, i.e. it is not subject to temporal changes being typical, for example, for real fingerprints (in particular, in connection with possible damage and/or contamination). In addition, holder 54 of device 42 provides very thin and stable combination of the biometric parameter image on the biometric key with the inlet surface of the readout sensor 57. Practice shows that one cannot reach similar stability in respect of user fingers, as at least a part of users are characterised by a low reproducibility of placing a finger on the readout sensor. On average, from 10% to 20% users have difficulties with dactyloscopic identification whereas the error level in case of application of the barometric key under this invention is significantly lower.

[0063] If as a result of search has been found, at least one verified electronic code matching the readout image code, device 42 will generate the corresponding (visual, audio and/or any other) signal on the identification taken place (operation 260). Otherwise a signal on the negative identification result will be issued. In parallel, the corresponding signal can also be given to any executive mechanism (mechanisms), for example, to a mechanism of automatic opening of a door into a room with controlled access.

[0064] It is evident that in case of the use of a biometric key with images of several parameters, all above-described operations of this stage will be repeated for all these images. At that, the symmetrical location of the biometric parameter images on the biometric key in respect of its centre allows to sufficiently simply provide the consecutive matching of specified images with the inlet optical surface of the readout sensor 54 by means of turning of the biometric key 20 around the axis passing through its centre perpendicular to the key plane.

[0065] Though the identification version being described provides, with high reliability, the confirmation of authenticity of the image presented in order to identify the user, it in essence does not identify the user itself but only the biometric key, which it represents, i.e. does not prevent a danger of presentation of the key not by the person, to whom this key was issued.

[0066] The alternative versions of the proposed method are free from this limitations, according to which both the selected biometric parameter and the biometric key are jointly used for the identification purposes. First an identification version will be considered, which can be implemented without calling the database.

[0067] In the given version, the identification stage 201 provides the execution, in any order, of the above-mentioned procedure 210 for obtaining of the electronic code of the readout image and procedure 220 for obtaining of the electronic code of the n\biometric parameter (see Fig. 7).

[0068] Procedure 220 consists of operations 222-228 similar to the described operation 212-218 but being executed at placing of a user finger carrying the selected biometric parameter into the readout unit 50. In order to provide the compatibility of the given version of implementation of the method with other alternative versions, it is expedient to use the same electronic code format at the execution of operations 216, 226 as at generation

WAVELYNX EX. 1003, Pg. 1605
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

of the verified electronic codes (during operation 118) or any other format permitting a possibility of comparison of electronic codes of the readout image and the readout biometric parameter with the verified electronic codes.

[0069] Upon termination of procedures 210 and 220, processor unit 60 of the identification device 42 performs operation 240 for comparison of the electronic code of the readout biometric parameter and the electronic code of the readout image. Upon results of this comparison, device 42 generates the corresponding (visual, audio and/or any other) signal on the identification taken place or on the identification failure.

[0070] Fig. 8 shows another version of implementation of the identification stage 202 providing the attraction of both the biometric parameter and its image with calling the database. This version, like version 201 shown in Fig. 6 and 7, includes procedures 210 and 220 for obtaining of electronic codes in combination of the described operation 240 for the comparison of these electronic codes and with the additional operation 250 for the search in the database for a verified electronic code coinciding, in essence, with the electronic code of the readout biometric parameter and/or readout image. In case of application of the given version, the increase of probability of the accurate identification can be reached not only by the conduction of identification by several biometric parameters and/or several images of these parameters but also with the use of several verified electronic codes corresponding to each or several biometric parameters out of the selected ones. It allows to make the identification probability being close to 100% and, accordingly, reduce the error probability practically to zero.

[0071] One should also note that the described versions of identification with the use of the optical image of the biometric parameter can be used in combination with other suitable identification methods, for example, by voice, secret personal identification number (PIN), password, etc. In particular, a high identification effectiveness with the use of this invention has been proved by its experimental verification conducted on a group of users being employees of the applicant-company of this invention with the use of biometric keys in the form of plastic cards carrying processed optical images of two fingers with symmetrical location of images in respect of the central point of the map. These keys have been used in combination with "live" fingerprints and personal numbers of the users being entered by them on the keyboard of the identification device 42.

[0072] For specialists in the given area, numerous modifications, which can be introduced into this invention without coming out beyond its limits, will be evident. Foe example, instead of fingerprints, any other biometric parameters can be used, which allow to generate and record their optical images. The biometric key body (except the image area) can be made from any strong and safe material; any shape providing a possibility of a tight contact of the image area or areas with the inlet surface of the readout sensor can be given to the keys. Though the described design of the sensor being capable to read out information directly from a finger or a biometric key seems to be preferable; for several versions of implementation of the invention, sensors designed for the operation only with biometric keys of various shape are also suitable.

[0073] The functions of the device for electronic copy processing in the subsystem for the manufacture of biometric keys, the subsystem for generation and storage of the verified electronic code database and the processor unit of the identification device can be made on the basis of a single central computer connected with wired or wireless communication lines with a device for generation of the image of the selected biometric parameter, with the device for recording of the image and with all identification subsystems. One or two readout sensors and one or two holders, one of which is optimised for installation of the biometric key into it, and the second one - for placing of the user finger, can be provided in the identification device.

[0074] The readout device being described can also be used as an image generation device. In addition, the readout device can be equipped by means providing a possibility to surely distinguish electronic codes being obtained from a real biometric parameter and from its optical image on the biometric key, for example, by the availability of the pulse (see US 3639905; WO 98/27509) or other physiological characteristics (as it is described in US 5719950). The availability of such means considerable reduces the probability of forgeries, i.e. contributes to further enhancement of the identification reliability.

Claims

1. User identification method providing a stage for biometric key manufacture and database generation and a stage for the conduction of identification, with the stage for biometric key manufacture and database generation including the following operations:

   (a) selection of the biometric parameter of an individual user, for example, a fingerprint;
   (b) generation of the optical image of the selected user biometric parameter out of the variety of users;
   (c) recording of the generated image with the selected scaling on a blank of the biometric key of the given user in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in the specified spectral interval;
   (d) generation and saving for permanent stor-

WAVELYNX EX. 1003, Pg. 1606
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

age in the selected format, of at least one verified electronic code of the selected biometric parameter in the form of a set of digital signals unambiguously matching the specified biometric parameter;
(e) repetition of operations (b), (c) and (d) for remaining users out of the variety of users with obtaining one biometric key each for every user and with generation of the database of verified electronic codes of the selected biometric parameters;

with the identification stage including the following operations:
(f) matching of the image on the biometric key of any user being identified out of the variety of users with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;
(g) readout of the above-mentioned image by the readout sensor with generation of the electronic code of the image in the format providing a possibility of comparison of the electronic code of the image with the verified electronic codes;
(h) search for a verified electronic code coinciding, in essence, with the electronic code of the readout image, and
(i) output of the user identification result on the basis of the search results.

2. Method as per claim 1, **characterized in that** it additionally includes the following operations:

(j) matching of the selected biometric parameter of the user being identified with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;
(k) readout of the above-mentioned biometric parameter with generation of the electronic code of the readout parameter in the format providing a possibility of comparison of the electronic code of the readout biometric parameter with the verified electronic codes;
(l) search for a verified electronic code coinciding, in essence, with the electronic code of the readout biometric parameter,

with the operation (i) additionally including the account of results of the operation (l).

3. User identification method providing a stage for biometric key manufacture and a stage for the conduction of identification, with the stage for biometric key manufacture including the following operations:

(a) selection of at least one biometric parameter of an individual user, for example, his/her fingerprint;
(b) generation of the image of the selected user biometric parameter out of the variety of users;
(c) recording of the generated image with the being equal or close to 1, on a blank of the biometric key of the given user in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in the specified spectral interval,
(e) repetition of operations (b), (c) for remaining users out of the variety of users with obtaining one biometric key each for every user;

with the identification stage including the following operations:
(f) matching of the image on the biometric key of any user being identified out of the variety of users with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;
(g) readout of the above-mentioned image by the readout sensor with generation of the electronic code of the image;
(j) matching of the selected biometric parameter with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being serisitive in the selected spectral interval;
(k) readout of the above-mentioned biometric parameter of the user being identified with generation of his/her electronic code in the format providing a possibility of comparison of this electronic code with the above-mentioned electronic code of the readout image;
(m) comparison of the electronic code of the readout biometric parameter and the electronic code of the readout image; and
(n) output of the user identification result based on the comparison of electronic codes of the readout biometric parameter and the readout image.

4. Method as per claim 3, **characterized in that**

for each user out of at least a part of the specified variety of users, at least two biometric parameters are being selected;

operations (b), (e), (f), (g) shall be performed for all images to be recorded on the specified user biometric key;

operations (j) and (k) shall be performed for all biometric parameters of the same user;

operation (m) shall be performed for electronic codes of all readout biometric parameters and all readout images;

operation (n) shall be performed on the basis

WAVELYNX EX. 1003, Pg. 1607
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

of the results of comparison of electronic codes of each readout biometric parameter and each readout image.

5. Method as per claim 3 or 4, **characterized in that** the biometric key manufacture stage additionally includes the operation:

(o) generating and saving for permanent storage of verified electronic codes for all selected biometric parameters of all users out of the variety of users in the form of a set of digital signals unambiguously matching the specified biometric parameters, with generation of the database of verified electronic codes of selected biometric parameters in the format providing a possibility of comparison of the electronic code of the readout biometric parameter with the verified electronic codes;

in addition, operation (n) consists of the comparison of the electronic codes of the readout biometric parameter and the readout image with the verified electronic codes, and the decision on the positive identification result shall be taken at the detection of a verified electronic code, which, in essence, coincides with the electronic code of the readout biometric parameter and/or readout image.

6. Method as per claim 4 or 5, **characterized in that** at least a part of specified verified electronic codes and images are generated by means of readout of at least one of the specified readout sensors made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval, selected biometric parameters and biometric keys of all users out of the variety of users.

7. User identification method including the following operations:

(f) matching of the image of the selected biometric parameter of an individual user, for example, his/her fingerprint, with the inlet optical surface of the readout sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval; at that the above-mentioned image has been formed on the biometric key of the given user in the area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval;
(g) readout of the above-mentioned image by the readout sensor with generation of the electronic code of the image;
(j) matching of the selected biometric parameter with the inlet optical surface of the reading sensor made on the basis of a multi-element photo-detector being sensitive in the selected spectral interval;
(k) readout of the above-mentioned biometric parameter with generation of the electronic code of the readout parameter in the format providing a possibility of comparison of this electronic code with the above-mentioned electronic code of the readout image,
(m) comparison of the electronic code of the readout biometric parameter and the electronic code of the readout image; and
(n) output of the user identification result based on the results of comparison of electronic codes of the biometric parameter and the readout image.

8. Method as per claim 7, **characterized in that**
each biometric key out of at least a part of the specified variety of biometric keys contains images of at least two selected biometric parameters on one user located central-symmetrically on the biometric key;
operations (f) and (g) shall be performed for all images contained on the specified biometric key;
operations (j) and (k) shall be performed for all selected biometric parameters of the same user;
operation (m) shall be performed for electronic codes of all readout biometric parameters and all readout images;
operation (n) shall be performed on the basis of the results of comparison of electronic codes of all readout biometric parameters and all readout images.

9. Method as per any of the previous claims, wherein the specified image is a binary black-and-white image.

10. Method as per any of the previous claims, wherein the fingerprint is selected as a biometric parameter.

11. Method as per claim 10, **characterized in that** the operation (b) for generation of the image additionally includes image processing providing the enhancement of reliability of results at the execution of operation (g) for comparison of the electronic code of the readout image with the verified electronic images.

12. Method as per claim 1, **characterized in that** the image processing includes generation of a fingerprint skeleton with constant line thickness not less than doubling the resolution of the readout sensor.

13. Method as per any of the previous claims, wherein

WAVELYNX EX. 1003, Pg. 1608
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

a plastic card is selected as a biometric key.

14. Method as per any of the previous claims, wherein at the readout of specified image the image area is illuminated from the side reverse in respect of the side, on which the specified image has been generated.

15. Method as per any of the previous claims, wherein a coded information is additionally recorded on the biometric key, for example, in the form of n-dimensional bar-code, with the dimensions of the coded information recording area being selected close to the image dimensions.

16. Method as per any of claims 2-6, wherein the operations (b), (f), (g), (j) and (k) are performed with the use of one readout sensor.

17. User identification device comprising

a readout unit containing at least one readout sensor equipped by a multi-element photo-detector being sensitive in the selected spectral interval of the optical range; in addition, the readout unit is made with a possibility of reading the image from a biometric key out of the variety of biometric keys, each of which is intended for identification of user out of the variety of users and contains an image area made from a material being semi-transparent in the selected spectral interval of the optical range, in which an image of the biometric parameter of the specified user has been generated with the selected scaling;

a lighter providing uniform illumination of the readout sensor by radiation in the selected spectral interval of the optical-range;

a holder for installation and fixation of any biometric key out of specified variety of keys with bringing of the image generated thereon into contact with the inlet sensitive surface of the readout sensor; and

a processor unit connected to the readout unit outlet and equipped by means for the generation of an electronic code of the readout image and by means for comparison of the electronic code of the readout image with other electronic codes with generation of the first signal in case of detection of coincidence of the electronic code of the readout image with any other electronic code and with generation of the second signal, if no above-mentioned coincidence has been detected.

18. Identification device as per claim 17, wherein the specified image is a binary black-and-white image.

19. Identification device as per claim 17 or 18 , wherein the scaling factor equals or close to 1.

20. Identification device as per any of claims 17-19, wherein the specified inlet optical surface of the readout sensor is made of optical fibre.

21. Identification device as per any of claims 17-20, wherein a fingerprint is the specified biometric parameter.

22. Identification device as per claim 21, wherein the specified image is a fingerprint skeleton with the constant line thickness not less than doubling the resolution of the readout sensor.

23. Identification device as per any of claims 17-22, wherein a plastic card is selected as the biometric key.

24. Identification device as per any of claims 17-23, wherein the lighter is made capable to illuminate the biometric key being installed into the holder from the side being reverse in respect of the side, on which the specified image has been generated.

25. Identification device as per any of claims 17-26, wherein a coded information, for example, in the form of an n-dimensional bar-code is additionally recorded on the specified biometric key; in addition, the readout unit and the processor unit are made with a possibility of reading of the specified coded information and its decoding respectively.

26. Identification device as per claim 25, wherein the coded information contains data on the user biometric parameter.

27. Identification device as per claim 25 or 26, wherein the image and the coded information are located on the biometric key in a single readout area, which dimensions are determined by the dimensions of the photo-detecting surface of the readout sensor but are separated spatially.

28. Identification device as per any of claims 25-27, wherein the image is located in the centre of the readout region and the coded information is located in the edge area of the readout region.

29. Identification device as per any of claims 17-28, wherein each of at least a part of specified variety of biometric keys contains images of at least two selected biometric parameters of one user located symmetrically in respect of the centre of specified biometric key; in addition, the device is made with a possibility of consecutive matching of all specified images with the inlet optical surface of the readout sensor by means of turning of the biometric key around the axis passing through its centre perpendicular to the key plane.

WAVELYNX EX. 1003, Pg. 1609
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

30. Identification device as per claim 29, wherein the specified images and/or the coded information are recorded by means of various printing facilities, for example, various paints being non-transparent and/or reflecting radiation in various spectral interval of the optical range.

31. Identification device as per any of claims 17-30, wherein the holder is made with an additional possibility of assurance of a contact between the biometric parameter and the specified inlet surface of the readout sensor, and the readout unit is made with an additional possibility of reading of the specified user biometric parameter.

32. Identification device as per claim 31, wherein the processor unit is made with a possibility of storage or reception of verified electronic codes of the selected biometric parameter in the form of a set of a set of digital signals, each of which unambiguously corresponds to the specified biometric parameter of one of the users out of variety of users, and the means for comparison of the given unit are made with a possibility of conduction of the comparison of the electronic codes of the readout image and the readout biometric parameter with the specified verified electronic codes.

33. User identification system containing the following:

means for recording at least of the optical image of one biometric parameter of an individual user out of the variety of users, for example, his/her fingerprint, on a blank of the biometric key in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval;
a subsystem for generation and storage of the database of verified electronic codes for each specified biometric parameter of every user out of the variety of users; and
at least one user identification device containing the following:

a readout unit containing at least one readout sensor equipped by a multi-element photo-detector being sensitive in the selected spectral interval of the optical range; in addition, the readout unit is made with a possibility of reading the image from a biometric key out of the variety of biometric keys, each of which is intended for identification of one user out of a group of users and contains the image area made from a material being semi-transparent in the selected spectral interval of the optical range, in which an image of the biometric parameter of the specified user has been generated with the scaling equal or close to 1,
a lighter providing uniform illumination of the readout sensor by radiation in the selected spectral interval of the optical range,
a holder for installation and fixation of any biometric key out of specified variety of keys with bringing of the image generated thereon into contact with the inlet sensitive surface of the readout sensor; and
a processor unit connected to the readout unit outlet and equipped by means for the generation of an electronic code of the readout image and the readout biometric parameter and by means for comparison of the electronic code of the readout image and/or the electronic code of the readout biometric parameter, with generation of the first signal in case of detection of coincidence, in essence, of the electronic code of the readout image with any other electronic code and with generation of the second signal, if no above-mentioned coincidence has been detected.

34. Identification system containing the following:

means for recording, with the scaling equal or close to 1, of least of the optical image of the biometric parameter of an individual user out of the variety of users, for example, his/her fingerprint, on a blank of the biometric key in the image area made from a material being semi-transparent in the selected spectral interval of the optical range, with the use of a printing means, for example, a paint being non-transparent or reflecting radiation in this spectral interval,
at least one user identification device made in accordance with any of Items 19-31.

35. Identification system as per claim 34, wherein it additionally contains a subsystem for generation and storage of the database of verified electronic codes of each specified biometric parameter of every user out of the variety of users, with the identification device being made in accordance with Item 32.

WAVELYNX EX. 1003, Pg. 1610
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

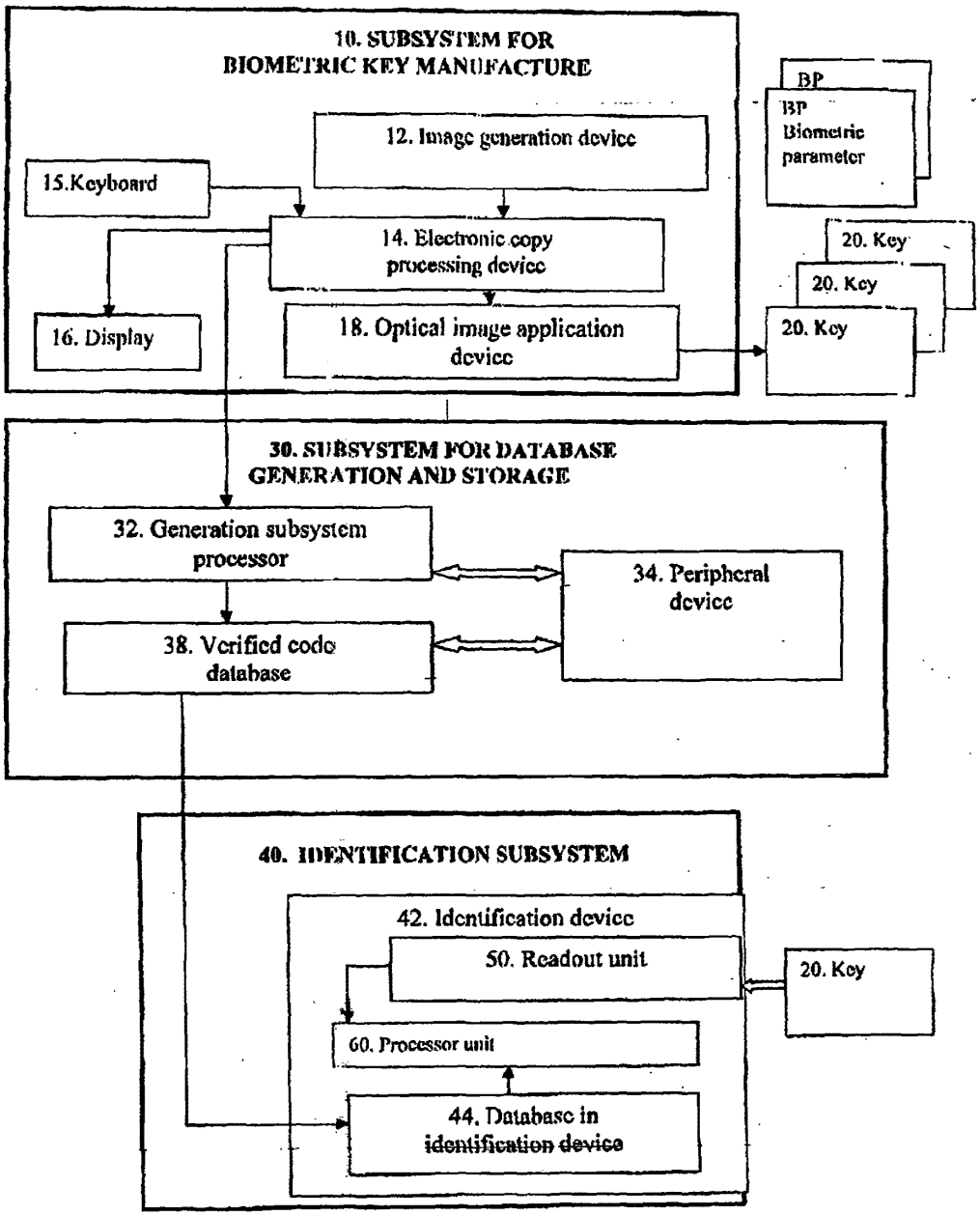


FIG. 1

WAVELYNX EX. 1003, Pg. 1611
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

42 Identification device

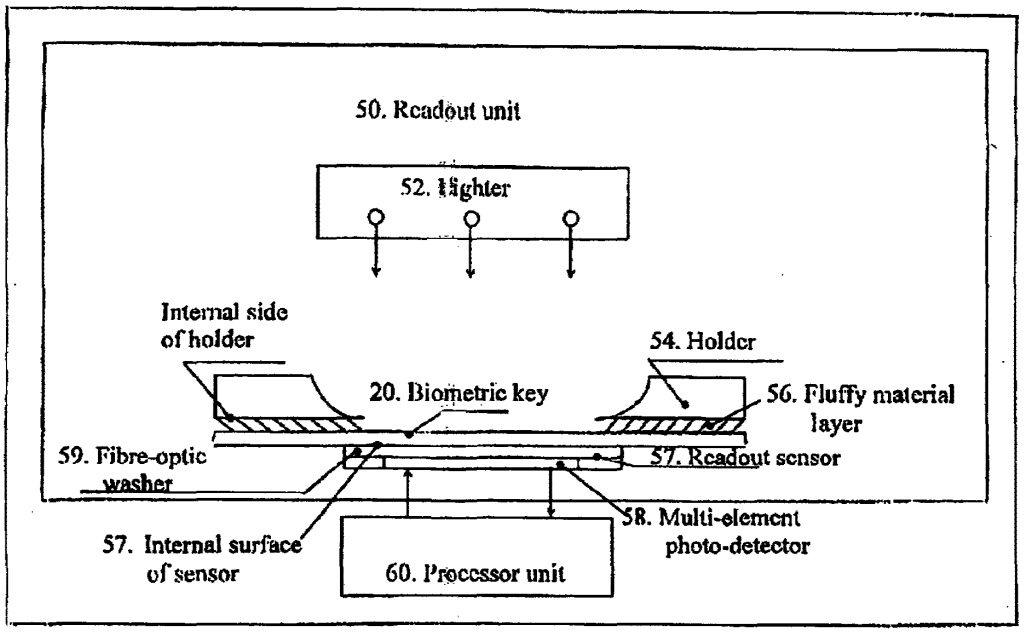


Fig. 3a

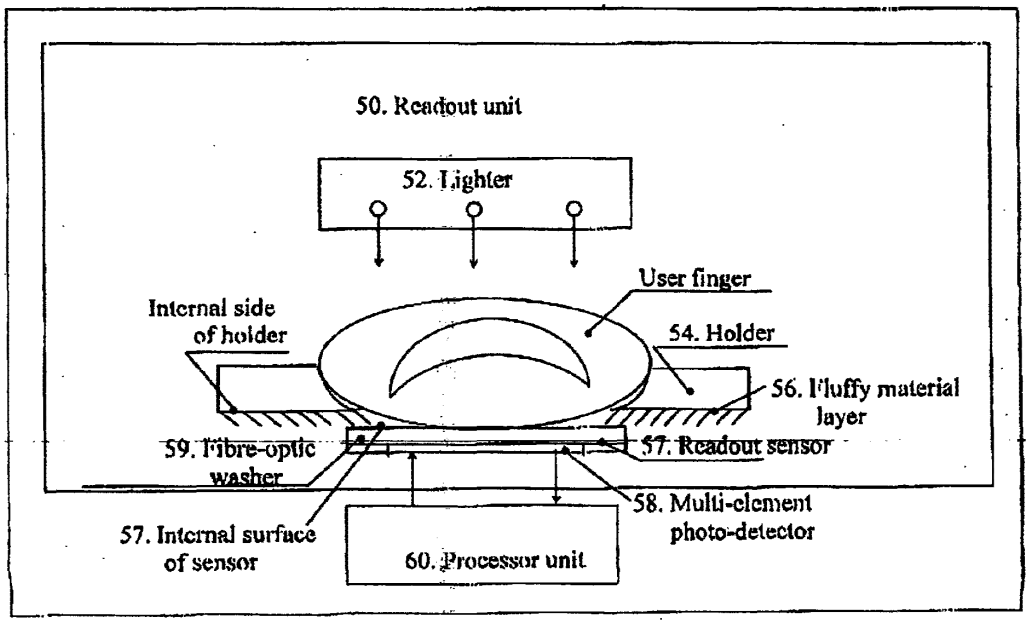


Fig. 3b

WAVELYNX EX. 1003, Pg. 1612
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

STAGE OF BIOMETRIC KEY MANUFACTURE

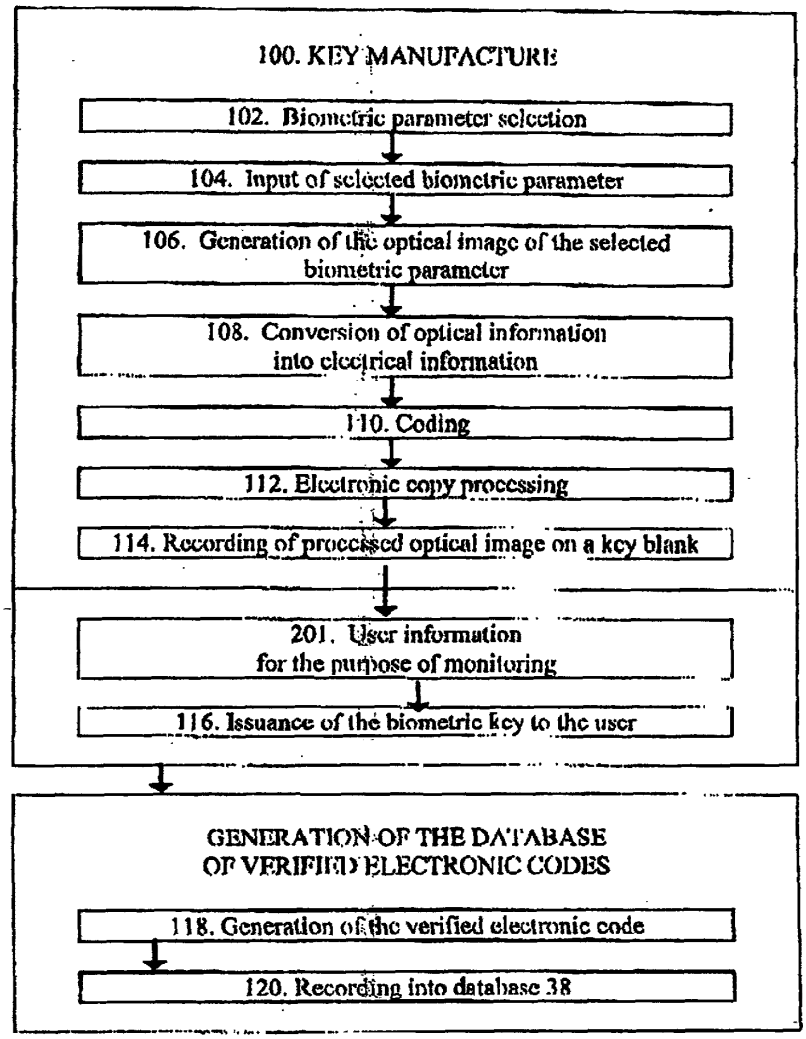


FIG. 4

WAVELYNX EX. 1003, Pg. 1613
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

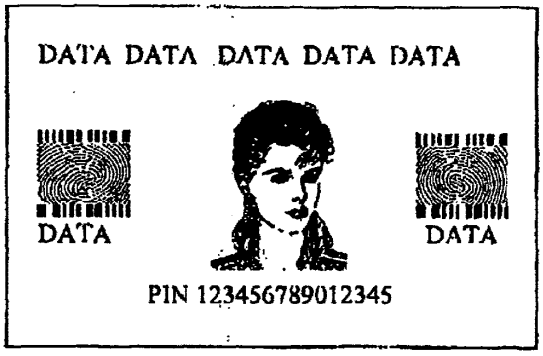


Fig. 2



Fig. 5A



Fig. 5B

WAVELYNX EX. 1003, Pg. 1614
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

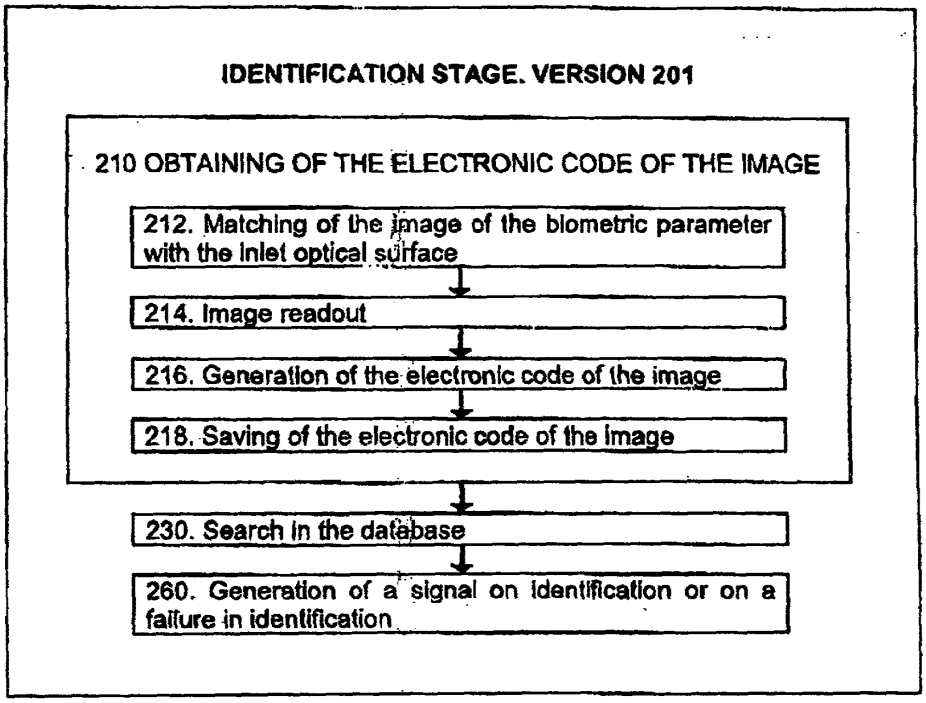


Fig. 6

WAVELYNX EX. 1003, Pg. 1615
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

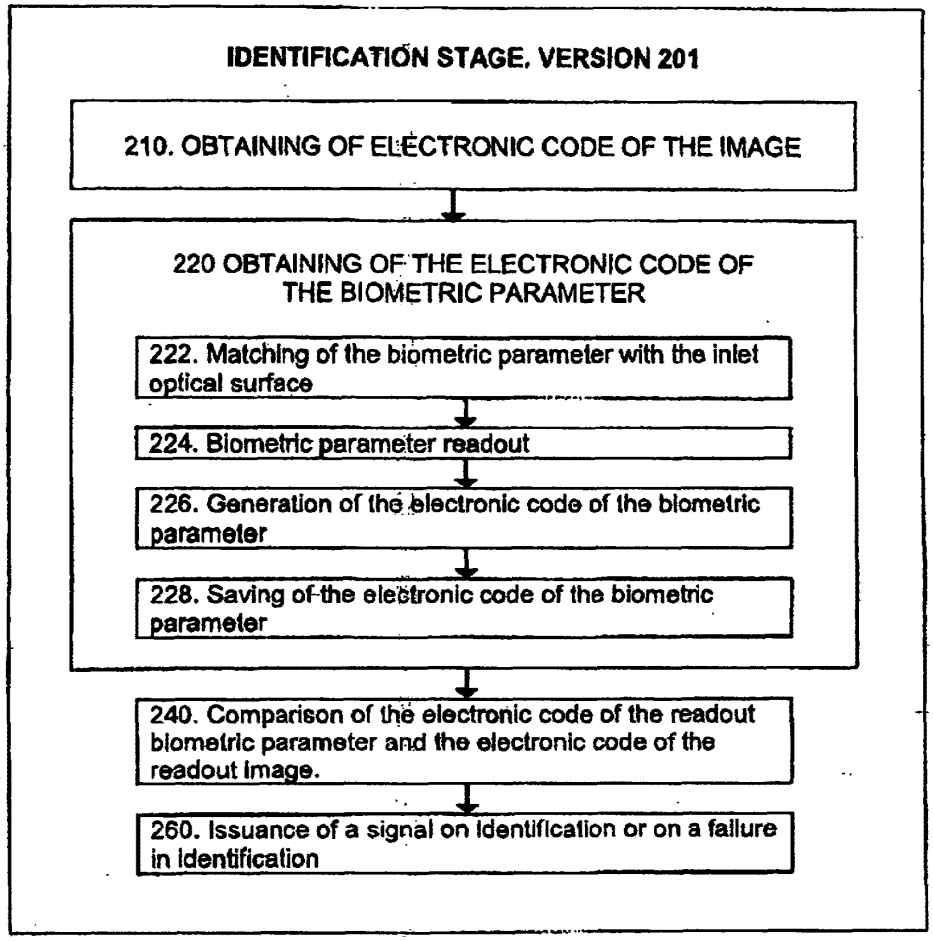


Fig. 7

WAVELYNX EX. 1003, Pg. 1616
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

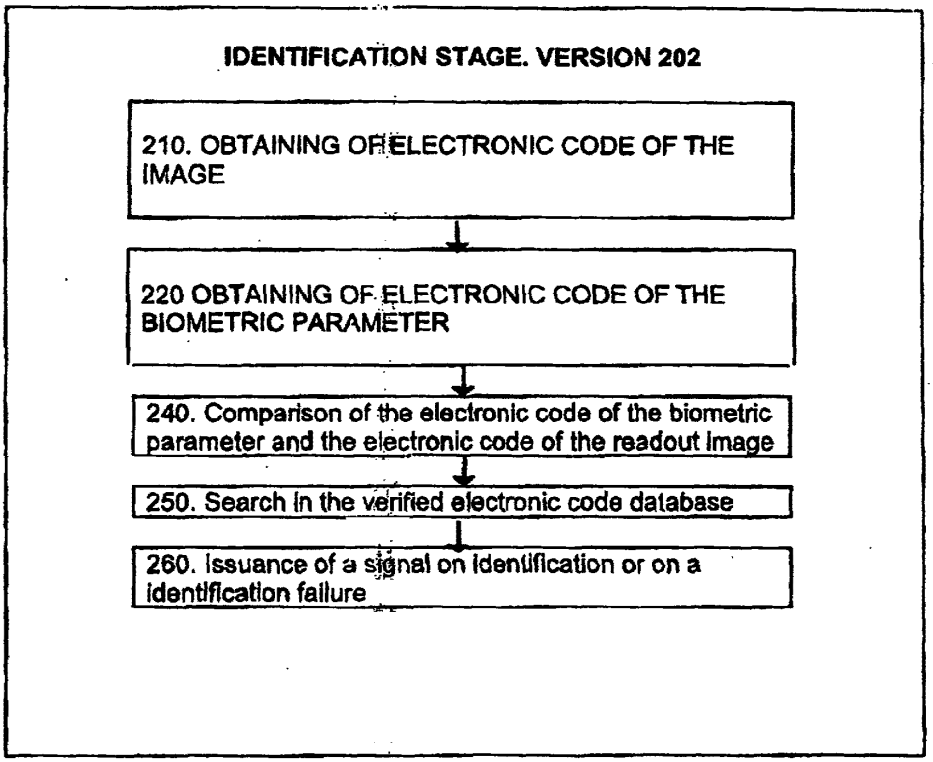


Fig. 8

WAVELYNX EX. 1003, Pg. 1617
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

International application No
PCT/ RU

A. CLASSIFICATION OF SUBJECT MATTER :
IPC 7 G06K 5/00, 19/00, G07F 7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K 5/00, 19/00, G07F 7/10, G07C 9/00, G06K 9/78, 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97/05578 A1 (MYTEC TECHNOLOGIES INC.) 13 February 1997 (13.02.97)	1 - 2
Y		3 - 6
X	US 5144680 A (MITSUBISHI DENKI KABUSHIKI KAISHA) 01 September 1992 (01.09.92)	17
X	WO 99/66448 A1 (IMAGEWARE SOFTWARE, INC.) 23 December 1999 (23.12.99)	1, 10, 17, 21, 23, 33 - 35
Y		4 - 7, 13

☒ Further documents are listed in the continuation of Box C ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search report	Date of mailing of the international search report
02 March 2001 (21.03.01)	05 April 2001 (05.04.01)
Name and mailing address of the ISA/RU Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

WAVELYNX EX. 1003, Pg. 1618
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

International application No.
PCT/RU 00/00446

C. (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4338025 A (ELTON D. ENGEL) Jul. 6, 1982	3-7, 13
A	US 5869822 A (DEXTER L. MEADOWS) Feb. 9, 1999	1-35

Form PCT/ISA/210 (continuation of second sheet) (July 1992) Page 2 of 2

WAVELYNX EX. 1003, Pg. 1619
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(12) UK Patent Application (19) GB (11) 2 256 170 (13) A

(43) Date of A publication 02.12.1992

(21) Application No 9209605.6

(22) Date of filing 05.05.1992

(30) Priority data
(31) 9109583 (32) 02.05.1991 (33) GB

(71) Applicant
William Robert Brandes
Little Thatch, 93 Middleton Road, Middleton on Sea, Bognor Regis, Sussex, PO22 6DW, United Kingdom

(72) Inventor
William Robert Brandes

(74) Agent and/or Address for Service
Michael Harrison & Company
22 The Grange Road, Leeds, LS16 6HA, United Kingdom

(51) INT CL[5]
G06K 9/00 19/07

(52) UK CL (Edition K)
B6A AC91 AK
G4R RRM R1X R10E R11D R11E R11F R9B

(56) Documents cited
GB 2185937 A WO 91/06920 A WO 90/12371 A
WO 82/03286 A US 4944021 A

(58) Field of search
UK CL (Edition K) B6A AK
INT CL[5] G06K
Online databases: WPI

(54) Integrated circuit card with fingerprint verification

(57) An integrated circuit or smart card stores encoded fingerprint data for verification purposes. The data is input into the card 9 using a biometric reader 1. At the point of use, a biometric reader (11, Fig. 2) interfaces with a card reader (13), the result of the comparison being displayed by printer (15).

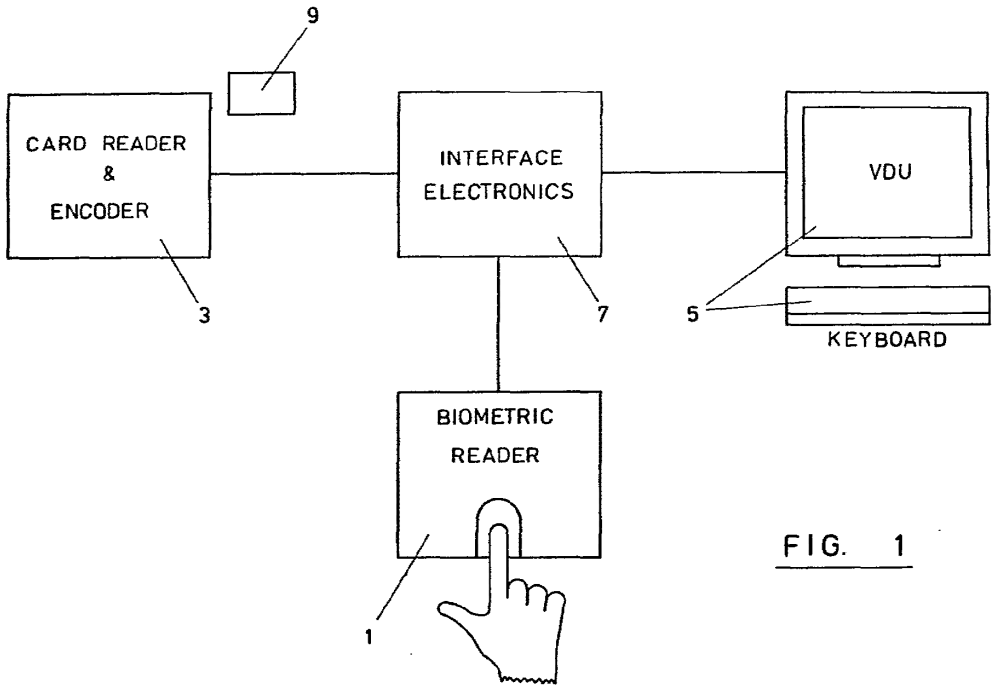


FIG. 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

GB 2 256 170 A

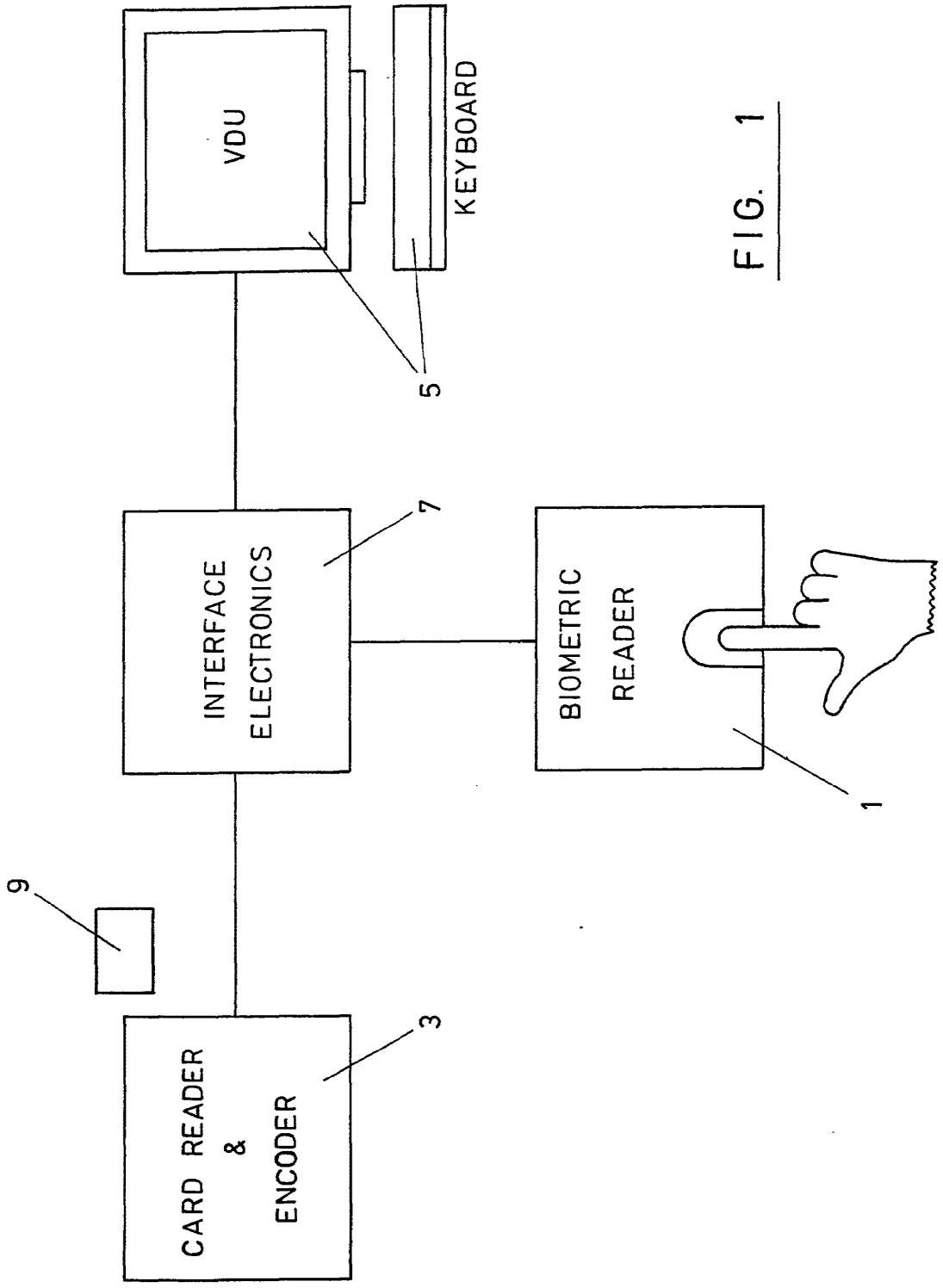

VDU
KEYBOARD
5
INTERFACE
ELECTRONICS
7
BIOMETRIC
READER
1
9
CARD READER
&
ENCODER
3

FIG. 1

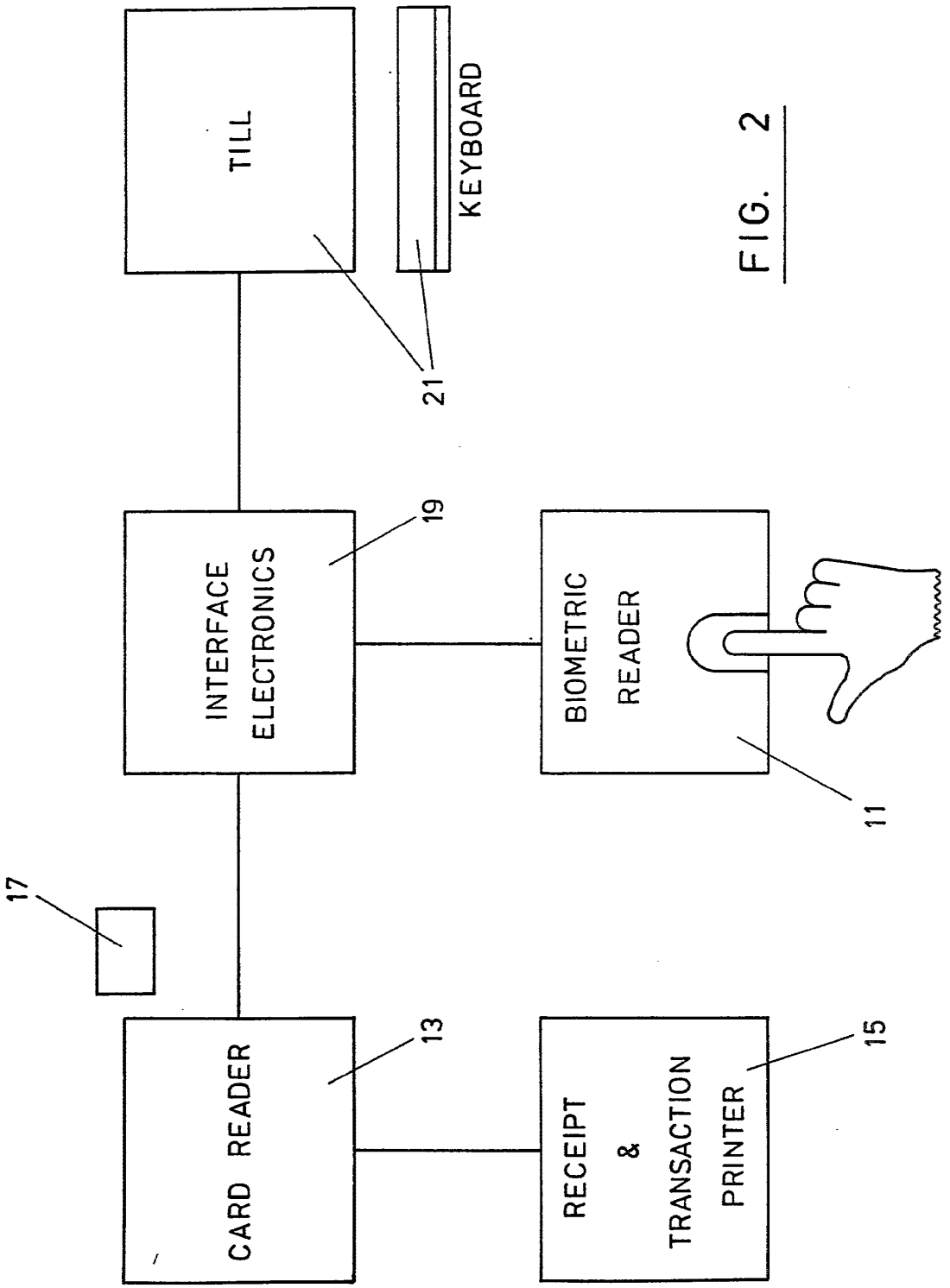

TILL
KEYBOARD
21
INTERFACE ELECTRONICS
19
BIOMETRIC READER
11
17
CARD READER
13
RECEIPT & TRANSACTION PRINTER
15

FIG. 2

2256170

ANTI-FRAUD IDENTIFICATION/PAYMENT CARD DEVICE

This invention relates to the prevention of fraud in the use of identification or payment cards, the term payment card including credit, debit and charge cards. For simplicity, reference will be made hereinafter to the term credit card although it should be understood that it includes all the above mentioned types of card.

An object of the invention is to reduce the incidence of credit card fraud in the particular case where a person other than the owner of the card has possession of it. It is frequently the case that such a person may attempt to obtain a financial or other advantage by presenting the card and, if necessary, reproducing the signature shown on the card.

According to the present invention there is provided a credit card which includes a device storing data characterising a fingerprint of the owner of the card, such a device being readable by appropriate data reading equipment.

The present invention also provides a method of preventing credit card fraud, the method comprising presenting the above defined card of the invention to a suitable data reading device, the apparent owner of the card then presenting a finger to fingerprint reading apparatus, which apparatus may be integral with the data reading device, the apparatus being arranged to compare the characteristics of the fingerprint with the data read from the credit card in order to verify that the possessor of the card is its rightful owner.

A credit card of the present invention may be the same as or similar to a so-called "smart" card which includes a data storage facility which may be wholly or partly loaded with data characterising a fingerprint.

An advantage of a device and method in accordance with the present invention is that there is no requirement for

WAVELYNX EX. 1003, Pg. 1623
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

sophisticated computer storage facilities, possibly remote from the apparatus at the point of use, nor to store details of fingerprints of all card holders. The fingerprint details are stored on the card itself and these are compared directly at the point of use with the appropriate fingerprint of the possessor of the card.

The fingerprint data which is stored on the card is unique to the rightful card owner and it cannot be in any way forged or tampered with. Utilisation is made of biometric techniques to analyse the card holder's fingerprint and to digitally encode unique aspects of this information onto the credit card. Up to a quarter of a million pieces of information may be analysed, digitised and converted to a unique mathematical characterisation. This does not entail the recording of a full fingerprint. It is only necessary to record a selection of pieces of information sufficient to provide uniqueness. It is not possible to print out this data as hard copy. A feature of the method of the present invention is that the data is not committed to any sort of computer memory or data base.

The present invention will now be described, by way of example only, with reference to the accompanying drawings in which:-

Figure 1 shows diagramatically the use of the present invention at the point of issue of the credit card; and

Figure 2 shows diagramatically the use of the present invention at the point of a sale.

Referring to Figure 1 of the accompanying drawings, a typical installation in, for instance, a bank or building society comprises a biometric reader 1 connected or interfaced to a magnetic card reader/encoder 3 and a keyboard/VDU 5 by means of interface electronics 7.

The card holder is issued with a credit card 9 which is encoded with fingerprint data at the point of issue, the card

WAVELYNX EX. 1003, Pg. 1624
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

holder's fingerprint being read, as indicated in Figure 1, by means of the biometric reader 1. In other words the card holder presents himself at his local issuing branch whereupon the live data will be read into the system by placing the forefinger onto the biometric reader 1. This data is automatically encoded onto the credit card 9 by the card encoder 3.

At the same time all other relevant data can be entered via the keyboard 5 and encoded on the card in the same way. All encoded data is then verified and the card is issued.

Referring now to Figure 2 of the accompanying drawings, a typical point of sale system comprises a biometric reader 11 interfaced to an online card reader 13 and receipt and transaction printer 15, the latter providing written confirmation of an "accept" or "deny" as a result of the biometric comparison as well as that of the credibility of the transaction being performed.

The card holder is required to place his forefinger on the biometric reader 11 in order to obtain data from the live finger which can be compared automatically with the data read from the card 17 by the card reader 13. The equipment includes interface electronics 19 which interfaces the above mentioned devices with cash till and keyboard 21.

The biometric reader 1 is arranged so that it will only read a "live" finger which exhibits warmth and detectable blood pressure, detectors being fitted in the equipment for this purpose.

CLAIMS

1. A credit card which includes a device storing data characterising a fingerprint of the owner of the card, such a device being readable by appropriate data reading equipment.

2. A credit card according to claim 1, the credit card being in the form of a "smart" card.

3. A method of preventing credit card fraud, the method comprising presenting a credit card, as defined in claim 1 or claim 2, to a suitable data reading device, the apparent owner of the card then presenting a finger to fingerprint reading apparatus, the apparatus being arranged to compare the characteristics of the fingerprint with the data read from the credit card in order to verify that the possessor of the card is its rightful owner.

4. A method according to claim 3 in which the data reading device is integral with the fingerprint reading apparatus.

5. A method according to claim 3 or claim 4 in which use is made of biometric techniques to analyse the card holder's fingerprint in order to produce a card suitable for use in the method.

6. A credit card according to claim 1 and substantially as herein described.

7. A method according to claim 3 and substantially as described herein with reference to the accompanying drawings.

F. .ents Act 1977
Examiner's report to the Comptroller under Section 17 (The Search Report)

Application number
9209605.6

Relevant Technical fields

(i) UK Cl (Edition K) B6A (AK)

(ii) Int Cl (Edition 5) G06K

Search Examiner
G J W RUSSELL

Databases (see over)

(i) UK Patent Office

(ii) ONLINE DATABASES: WPI

Date of Search
28 JULY 1992

Documents considered relevant following a search in respect of claims 1-7

Category (see over)	Identity of document and relevant passages	Relevant to claim(s)
X	GB 2185937 A (O'SHEA) - see whole document	1 and 2
X	WO 91/06920 (TMS) - see page 36 line 33 - page 38 line 3	1-5
X	WO 90/12371 (PERSONNEL) - see page 1 lines 18-20	1-5
X	WO 82/03286 (LOFBERG) - see whole document	1 and 2
X	US 4944021 (NEC) - see column 6 lines 10-37	1-5

WAVELYNX EX. 1003, Pg. 1627
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Category	Identity of document and relevant passages	Relevant to claim(s)

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family, corresponding document.

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).

Published 1992 at The Patent Office, Concept House, Cardiff Road, Newport, Gwent NP9 1RH. Further copies may be obtained from Sales Branch, Unit 6, Nine Mile Point, Cwmfelinfach, Cross Keys, Newport, NP1 7HZ. Printed by Multiplex techniques ltd, St Mary Cray, Kent.

(12) UK Patent Application (19) GB (11) 2 331 825 (13) A

(43) Date of A Publication 02.06.1999

(21) Application No 9826116.7

(22) Date of Filing 27.11.1998

(30) Priority Data
(31) 09328546 (32) 28.11.1997 (33) JP

(51) INT CL[6]
G06F 1/00 12/14 , G07F 7/10 19/00

(52) UK CL (Edition Q)
G4H HTG H1A H13D H14A
U1S S2125 S2132

(56) Documents Cited
EP 0379333 A1 WO 94/10659 A1 US 4993068 A

(58) Field of Search
UK CL (Edition P) G4H HTG
INT CL[6] G06F , G07C , G07F

(71) Applicant(s)
NEC Corporation
(Incorporated in Japan)
7-1 Shiba 5-chome, Minato-ku, Tokyo 108, Japan

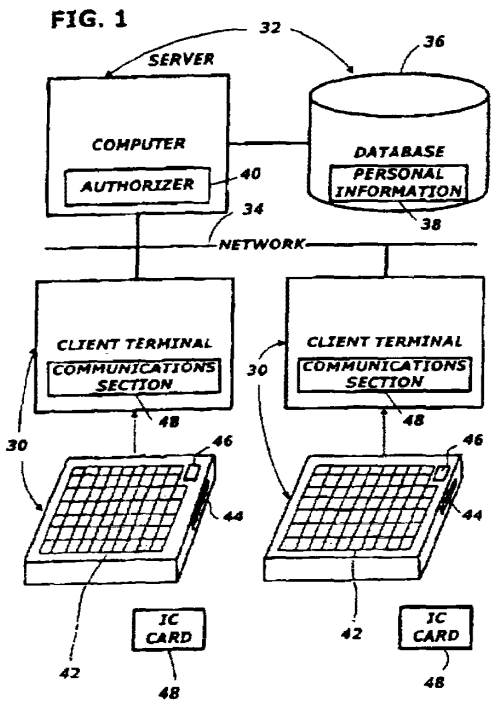
(72) Inventor(s)
Satoshi Hoshino

(74) Agent and/or Address for Service
Mathys & Squire
100 Grays Inn Road, LONDON, WC1X 8AL,
United Kingdom

(54) Abstract Title
Personal identification authentication using fingerprints

(57) A personal identification authenticating system for a client terminal 30 in communication with a server 32 is disclosed. The server includes a computer and a database which stores personal information of the service users including information related to fingerprints and ID numbers of the service users. A client terminal user impresses his fingerprint on a fingerprint sensor 46 and puts his IC card 48 into a card reader 44. The IC card stores personal information including information related to a fingerprint and an ID number of the card owner. The client terminal includes an authenticator, which provides an authenticating signal if the sensed fingerprint information matches stored fingerprint information from the card. The client terminal transmits stored personal information from the card and the sensed fingerprint information to the server upon occurrence of the authenticating signal. The server incorporates an authorizer 40. The authorizer transmits an authorizing signal to the client terminal if the transmitted information matches the stored personal information on the database. Upon receiving the authorizing signal, the client terminal user is authorized to access into the computer of the server.

FIG. 1



GB 2 331 825 A

BNSDOCID: <GB___2331825A__I_>

PERSONAL IDENTIFICATION AUTHENTICATING WITH FINGERPRINT IDENTIFICATION

FIELD OF THE INVENTION

The present invention relates to a system for authenticating personal identification and more particularly to a personal identification authenticating system for a client terminal in communication with a server.

BACKGROUND OF THE INVENTION

Proving one's identify is necessary when accessing a computer whose users are limited. In order to prevent individuals other than the registered users from accessing the computer, a password or a personal identification number is issued with each ID card. Access to the computer is enabled only when both a password and an ID number corresponding to the user's number read from the ID card is entered through the keyboard.

Transaction execution systems which enable the performance of transactions, such as cash issuance at terminals remote from and in communication with a host data processing system having a central database in which account and other information is stored, are well known.

Such systems, which are frequently used by banks to extend their services, permit the issuance of cash or the receipt of deposits through a terminal, for example, an automatic teller machine (ATM). Such a terminal typically includes a mechanism for receiving and reading information from a card, a user input such as a keyboard, a display and document entry and exit apertures. Issuing a personal ID number with each credit card attains increased security for the issuance of cash or other banking transactions without intervention of a bank employee. A credit card transaction is then enabled only when an ID number corresponding to the

WAVELYNX EX. 1003, Pg. 1630
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

account number read from the credit card is entered through the keyboard. This required correspondence prevents a thief or mere finder of a credit card from receiving cash, for example, from a terminal. Upon entry by a terminal user or a customer of a credit card and personal identification number, the terminal is instructed to communicate the credit card data and the personal identification number to the host for authorization of the transaction. At the host, a database of identification numbers is accessed by the card data. The identification number obtained from the database is compared with the personal identification number received from the terminal to perform a host PIN check.

When ID cards, credit cards or other cards are stolen, passwords and/or ID numbers read from cards are decrypted. Thus, presenting a password or a personal identification number with a card is woefully inadequate in preventing individuals other than the registered users from accessing the computer.

It is known to use fingerprints in conjunction with an identification card to verify ownership of the card. JP-A 63-288365 discloses an ATM wherein a selector button to be pressed by a customer for transaction is transparent. A fingerprint of the customer impressed on this transparent button is recorded using optical system including a video camera. The recorded fingerprint information is compared with stored fingerprint information.

JP-A 1-154296 discloses an ATM wherein a selector button, such as a yen key, is provided with a fingerprint pickup head of an optical fingerprint recording system.

Various compact fingerprint sensors are disclosed by US-A 5,446,290 (issued on August 29, 1995) that is considered to correspond to JP-A 6-325158, US-A 5,635,723 (issued on June 3. 1997) that is considered to correspond to JP-A 8-380173,

WAVELYNX EX. 1003, Pg. 1631
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

and US-A 5,708,497 (issued on January 13, 1998) that is considered to correspond to JP-A 9-136328.

In transaction execution systems, a transaction terminal is designed for maximum likelihood that the user of the terminal can perform the transaction in an error free manner even if the use has never operated the terminal before. Such a terminal typically includes a group of selector buttons which allow the customer to perform the transactions and a keypad which may be used the customer to enter money amounts. Thus, the selector or key switches or buttons of the terminal do not exceed a certain number in the neighborhood of 40. The transaction terminal may include a supply of cash and a cash dispensing mechanism and may also include a depository for receiving customer deposits. These components would then be located within the security chest. In addition, the main control electronics for the terminal may also be located within the security chest so as to prevent any unauthorized access to the control electronics. In addition to the components of the terminal system located within the security chest, a number of components may be located outside the security chest. Thus, the terminal is not compact. In the transaction execution systems, a highly reliable communication means such as an exclusive line is used to establish communication between each terminal with the host data processing system.

In a local area network (LAN) or a wide area network (WAN), personal computers and workstations are used as terminals. Internet system with great number of servers and clients allows the use of desktop or hand-held terminals. A keyboard of such a terminal includes a great number of key or selector switches that amount in number to approximately 300. In the internet systems, each server may perform an exclusive service for a group of authorized users and also may

BNSDOCID: <GB___2331825A__I_>

perform an open service whose users are unlimited. Communication means used to connect each terminal to such a server is not highly reliable.

It would therefore be desirable to provide a personal identification authenticating system for use in a terminal that can request both an exclusive service and an open service to a server. The exclusive service requires authentication of personal identification of the terminal user before access to a computer of the server although the free service requires password only from the terminal user.

An object of the present invention is to provide a small-sized personal identification authenticating system for preventing unauthorized individuals from accessing a computer.

SUMMARY OF THE INVENTION

According to one aspect of the present invention, there is provided a system for authenticating personal identification, comprising:

a server including a computer whose users are limited, said server having a database storing information related to ID numbers assigned to said users and information related to fingerprints of said users;

an IC card storing personal information including information related to an ID number of the card owner and information related to a fingerprint of the card owner;

a client terminal in communication with said server, said client terminal including a card reader for reading the stored personal information on said IC card, and a fingerprint sensor for sensing a fingerprint of the client terminal user;

an authenticator that compares the sensed fingerprint information of the client terminal user with the stored fingerprint information of the card owner and produces an authentication signal if the sensed fingerprint information

WAVELYNX EX. 1003, Pg. 1633
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

matches the stored fingerprint information;

a transmitter that transmits personal information including the sensed fingerprint information and the authentication signal to said server if the authentication signal is produced; and

an authorizer that compares the transmitted personal information of the card owner with the stored personal information on the database and produces an authorization signal if the transmitted personal information matches the stored information on the database, thereby to give the client terminal user an access to said computer of said server.

According to another aspect of the present invention, there is provided a method of authenticating personal identification for a client terminal in communication with a server that includes a computer and a database, the method comprising the steps of:

storing into the database information related to identification numbers and fingerprints of users who are allowed to access into the computer of the server;

storing into an IC card information related to an identification number and a fingerprint of each of the users;

presenting descriptive screen to a client terminal user to give instructions to the client terminal user;

sensing a fingerprint of the client terminal user;

reading the stored information on the IC card;

comparing the sensed fingerprint information with the stored fingerprint information of the card owner;

transmitting the sensed fingerprint information of the client terminal user and the stored information of the card owner to the server from the client terminal if the sensed fingerprint information matches the stored fingerprint information of the card owner;

comparing the transmitted information with the stored

WAVELYNX EX. 1003, Pg. 1634
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

information on the database; and

authorizing the client terminal use to access into the computer if the transmitted information matches the stored information on the database.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates client terminals in communication with a server incorporating a personal identification authenticating system according to the present invention.

Figure 2 is a block diagram of the terminal.

Figure 3 is a perspective view partially broken away of a fingerprint sensor.

Figure 4 is a flow chart illustrating a method of authenticating personal identification.

Figure 5 illustrates a terminal and a server, in the form of a single computer incorporating the personal identification authenticating system according to the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. The terms "server," "client terminal," and "integrated circuit (IC) card" are used throughout the specification. The term "server" is meant to include a data processing system that performs a service for clients. The term "client terminal" is meant to include a terminal that requests services of a server. The term "IC card" is used to mean cards that can store personal information including information related to a fingerprint of the card owner, and is meant to include cards whose purpose is purely identification, and diverse other cards used for additional purposes as well.

Referring to Figure 1, the personal identification authenticating system is designed to authenticate identification of a user of each client terminal 30. The client terminals 30

WAVELYNX EX. 1003, Pg. 1635
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

are in communication with a server 32 through a network 34. The server 32 includes a computer. In this embodiment, the server 32 can perform both an exclusive service whose users are limited and an open service whose users are unlimited although it may perform an exclusive service only.

The server 32 includes a database 36 storing personal information 38. The personal information 38 includes information related to ID numbers and fingerprints of users authorized to access the computer of the server 32. The server 32 also includes an authorizer 40, which compares personal information transmitted from a client terminal 30 with the stored personal information 38 on the database 36. The authorizer 40 transmits an authorization signal to the client terminal 30 if the transmitted personal information matches the stored personal information 38 on the database 36.

Each client terminal 30 includes a user input device in the form of a keyboard 42, an IC card reader 44, and a fingerprint sensor, preferably in the form of a semiconductor fingerprint sensor 46 (see Figure 3). It also includes a communications section 48 for transmitting and receiving information to and from the server 32. The fingerprint sensor may sense information related to a fingerprint using a multiple of small capacitors to detect the ridges and valleys of a fingerprint. A client terminal user puts an IC card 48 into a slot of the IC card reader 44. Each IC card 48 stores personal information of the card owner. The stored personal information includes information related to an ID number of the card owner and information related to a fingerprint of the card owner. It is preferred that the fingerprint information be encrypted.

The client terminal 30 as illustrated in Figure 2 carries in addition to the IC card reader 44 and the fingerprint sensor 40, and an authenticator 48. The authenticator 48 is

WAVELYNX EX. 1003, Pg. 1636
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

electrically connected to the finger print sensor 46 and the IC card reader 44. It compares information related to a sensed fingerprint with the stored fingerprint information on the IC card 48 and produces an authentication signal if the sensed fingerprint information matches the stored fingerprint information. A transmitter 50 is electrically connected to the IC card reader 44 and the fingerprint sensor 46 for transmitting the sensed fingerprint information, the personal information read by the IC card reader 44 and the authenticating signal to the server 32 only if the authenticating signal has been produced. A receiver 52, for receiving an authorization signal from the server 32, and a display 54, for indicating that a client terminal user has been approved for accessing the computer of the server 32, are preferably included in the client terminal 30. The keyboard 42 is used by the terminal user for entering information. The transmitter 50 is rendered responsive to the keyboard 42 for transmitting information entered by the keyboard 42 to the computer of the server 32 upon or after receipt of the authorizing signal from the server 32. A controller 56 controls operations of the client terminal 30.

The server 32 includes an access approval mechanism for receiving the personal information including the sensed fingerprint information along with the authenticating signal to compare this personal information with the stored personal information 38 from the database 36 and for approving access to the computer of the server 32. Specifically, the authorizer 40 transmits an authorizing signal to the client terminal 30 if the personal information transmitted from the client terminal 30 matches the stored personal information 38 on the database 36. The authorizer 40 may transmit its signals over the network 34.

Referring now to Figure 3, the fingerprint sensor 46 of

BNSDOCID <GB___2331825A__I_>

Figures 1 and 2 will be described. The fingerprint sensor 46 of the illustrated type is disclosed in US-A 5,446,290 issued on Aug. 29, 1995 to Fujieda et al., the disclosure of which is incorporated in its entirety herein by reference. Briefly explaining, the fingerprint sensor 46 includes a planar light source 11, a two-dimensional image sensor 12, and optical element 13. The two-dimensional image sensor 12 includes a great number of photosensitive elements 24 arranged two-dimensionally on a transparent substrate 21. Each photosensitive element 24 is formed on a light shielding plate 23 and connected to a terminal of a signal reading switch 22 in the form of a polycrystalline silicon thin film transistor (TFT). The switch 22 is further connected to a signal reading line 26 and a switching line 25. The photosensitive elements 24 arranged along the switching line are connected to a bias applying line 27. An opening 28 is provided in an area unoccupied by the lines 25, 26 and 27 and the light shielding plates 23.

A preferred method of authenticating personal identification is illustrated by the flow chart of Figure 4. After activation of a client terminal 30, a descriptive screen is presented or shown by step S1. This screen offers a client terminal user instructions to put an IC card 48 into a slot of an IC card reader 44 and place a fingerprint on a fingerprint sensor 46. In accordance with the instructions on the descriptive screen, the user puts an IC card 48 into the slot of the IC card reader 44 and places a fingerprint on the fingerprint sensor 46 by step S2. Information related to the fingerprint is sensed and the stored personal information is read by step S3. The sensed fingerprint information is compared with the stored fingerprint information by step S4 to determine if there is a match. The comparison result is checked by step S5. If there is a match, the sensed

WAVELYNX EX. 1003, Pg. 1638
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

fingerprint information by the fingerprint sensor 46 and the stored personal information read by the IC card reader 44 are transmitted from the terminal 30 to a serve 32 along with an authenticating signal by step S6. At the server 32, the transmitted personal information including the sensed fingerprint information is compared with the stored personal information 38 on a database 36 by step S7. If the transmitted information by the client terminal 30 matches the stored information on the database 36, an authorization signal is transmitted to the client terminal 30 by step S8. If there is no match, a rejection signal or no signal is transmitted to the client terminal 30 by step S9. If, at step S5, there is no match between the sensed fingerprint information and the stored fingerprint information, an access reject message is presented or shown by step S10. In this case, the information will not be transmitted from the client terminal 30 to the server 32. This reduces load carried by the server 32 and the network 34.

From the preceding description, it is noted that the sensed fingerprint information, which has been compared with the stored fingerprint information, is transmitted to the server 34 along with the authenticating signal for comparison with the stored information 38 on the database 36. This authenticates personal identification of a client terminal user with a high degree of accuracy and security even if the network 34 is not highly trustworthy.

Figure 5 illustrates a terminal 30A connected a server in the form of a single computer 32 by a highly reliable communication line 34A. The same reference numerals as used in Figures 1 and 2 are used in Figure 5 to designate like or similar parts. The system illustrated Figure 5 may incorporate the personal identification authenticating system thus far described without any substantial modification.

If communications between client terminals and each

BNSDOCID: <GB___2331825A__I_>

server are highly reliable and trustworthy like the one illustrated in Figure 5, the sensed fingerprint information may be transmitted directly to the server for comparison with stored data on a database of the server.

If client terminal users are authenticated with a high degree of accuracy and security, a server is enabled to perform such exclusive services as application software logon, encryption of application data, decryption of data with encrypted key and electronic signature and its verification with a high degree of security.

Once one is authorized as a user of an exclusive service performed by a server that performs various other open services, this user may request such services to this server through any one of client terminals that have incorporated the personal identification authenticating system according to the present invention.

Each feature disclosed in this specification (which term includes the claims) and/or shown in the drawings may be incorporated in the invention independently of other disclosed and/or illustrated features.

Statements in this specification of the "objects of the invention" relate to preferred embodiments of the invention, but not necessarily to all embodiments of the invention falling within the claims.

The description of the invention with reference to the drawings is by way of example only.

The text of the abstract filed herewith is repeated here as part of the specification.

BNSDOCID: <GB___2331625A__I_>

A personal identification authenticating system for a client terminal in communication with a server is disclosed. The server includes a computer and a database. The server performs a service whose uses are limited. In the system, the client terminal plays a role of an IC card authorizing device, while the server plays a role of an approval center. The database stores personal information of the service users. The stored personal information on the database includes information related to fingerprints and ID numbers of the service users. A client terminal user impresses one's fingerprint on a fingerprint sensor and puts one's IC card into a card reader. The IC card stores personal information of a card owner. The stored personal information on the IC card includes information related to a fingerprint and an ID number of the card owner. The client terminal includes an authenticator, which provides an authenticating signal if the sensed fingerprint information of the client terminal user matches stored fingerprint information of the card owner. The client terminal transmits the stored personal information of the card owner to the server upon occurrence of the authenticating signal. The server incorporates an authorizer. The authorizer transmits an authorizing signal to the client terminal if the transmitted personal information of the card owner matches the stored personal information on the database. Upon receiving the authorizing signal, the client terminal user is authorized to access into the computer of the server.

BNSDOCID: <GB___2331825A__I_>

WAVELYNX EX. 1003, Pg. 1641
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

WHAT IS CLAIMED IS:

1. A system for authenticating personal identification, comprising:

a server including a computer whose users are limited, said server having a database storing information related to ID numbers assigned to said users and information related to fingerprints of said users;

an IC card storing personal information including information related to an ID number of the card owner and information related to a fingerprint of the card owner;

a client terminal in communication with said server, said client terminal including a card reader for reading the stored personal information on said IC card, and a fingerprint sensor for sensing a fingerprint of the client terminal user;

an authenticator that compares the sensed fingerprint information of the client terminal user with the stored fingerprint information of the card owner and produces an authentication signal if the sensed fingerprint information matches the stored fingerprint information;

a transmitter that transmits personal information including the sensed fingerprint information and the authentication signal to said server if the authentication signal is produced; and

an authorizer that compares the transmitted personal information of the card owner with the stored personal information on the database and produces an authorization signal if the transmitted personal information matches the stored information on the database, thereby to give the client terminal user an access to said computer of said server.

2. The system as claimed in claim 1, wherein said server

WAVELYNX EX. 1003, Pg. 1642
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

performs both an exclusive service whose users are limited and an open service whose users are unlimited.

3. The system as claimed in claim 1, wherein the stored fingerprint information on the IC card is encrypted.

4. The system as claimed in claim 1, wherein said fingerprint sensor is a semiconductor fingerprint sensor.

5. A method of authenticating personal identification for a client terminal in communication with a server that includes a computer and a database, the method comprising the steps of:

storing into the database information related to identification numbers and fingerprints of users who are allowed to access into the computer of the server;

storing into an IC card information related to an identification number and a fingerprint of each of the users;

presenting descriptive screen to a client terminal user to give instructions to the client terminal user;

sensing a fingerprint of the client terminal user;

reading the stored information on the IC card;

comparing the sensed fingerprint information with the stored fingerprint information of the card owner;

transmitting the sensed fingerprint information of the client terminal user and the stored information of the card owner to the server from the client terminal if the sensed fingerprint information matches the stored fingerprint information of the card owner;

comparing the transmitted information with the stored information on the database; and

authorizing the client terminal use to access into the computer if the transmitted information matches the stored information on the database.

BNSDOCID: <GB___2331825A__I_>

6. The method as claimed in Claim 5, further comprising the step of:

presenting access reject message to the client terminal user if the sensed fingerprint information fails to match the stored fingerprint information of the card owner.

7. The method as claimed in Claim 5, wherein the server performs both an exclusive service whose users are limited and an open service whose users are unlimited.

8. A system or a method substantially as herein described with reference to the accompanying drawings.

BNSDOCID: <GB___2331825A__I_>

The Patent Office

16

Application No: GB 9826116.7 **Examiner:** Mike Davis
Claims searched: 1-8 **Date of search:** 15 December 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): G4H (HTG)

Int Cl (Ed.6): G06F, G07F, G07C

Other:

Documents considered to be relevant:

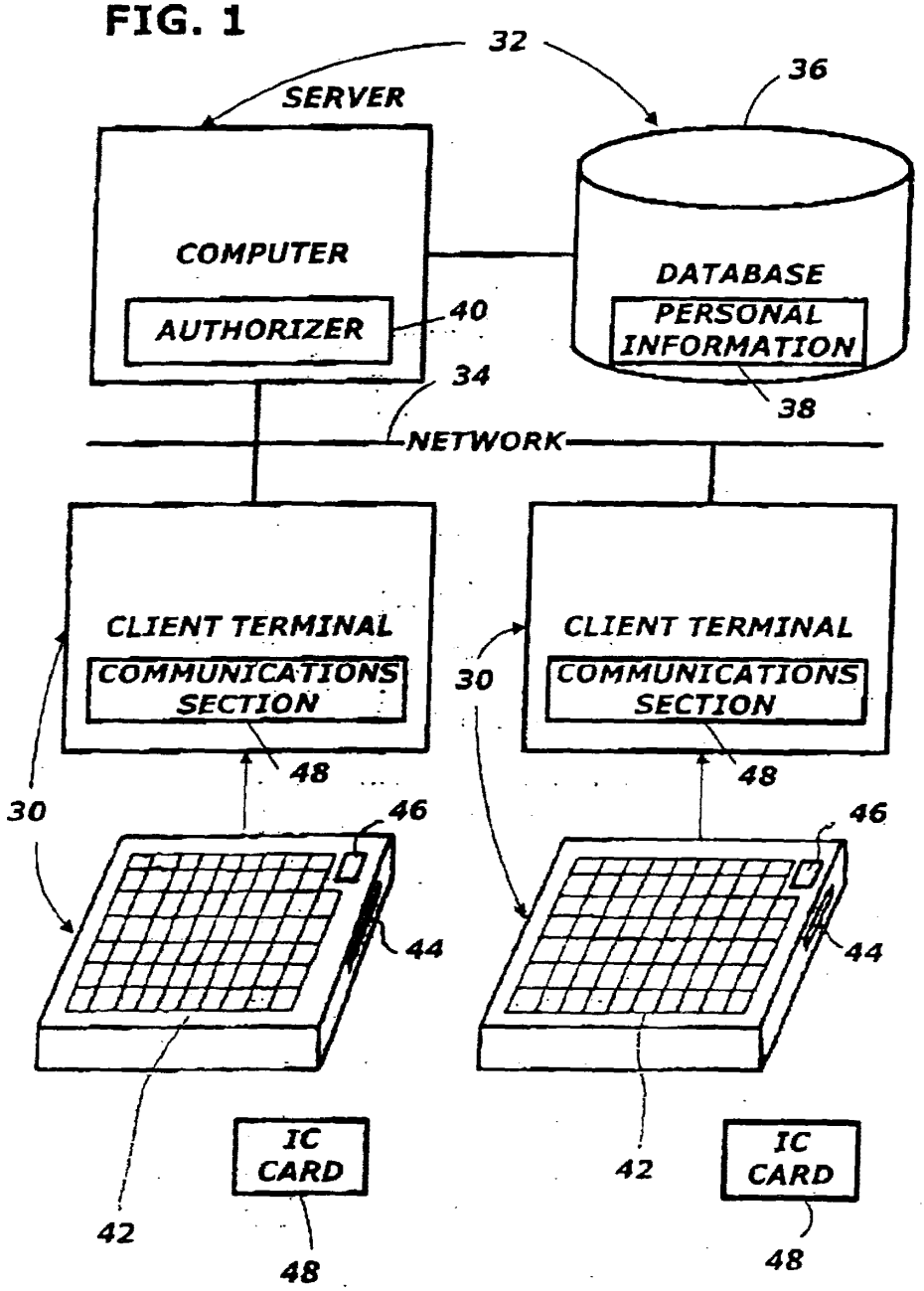
Category	Identity of document and relevant passage		Relevant to claims
A	EP 0379333 A1	(GRAVES) eg abstract	-
A	WO 94/10659 A1	(JASPER CONSULTING) eg abstract	-
A	US 4993068	(PIOSENKA ET AL) eg abstract	-

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB___2331825A__!_>

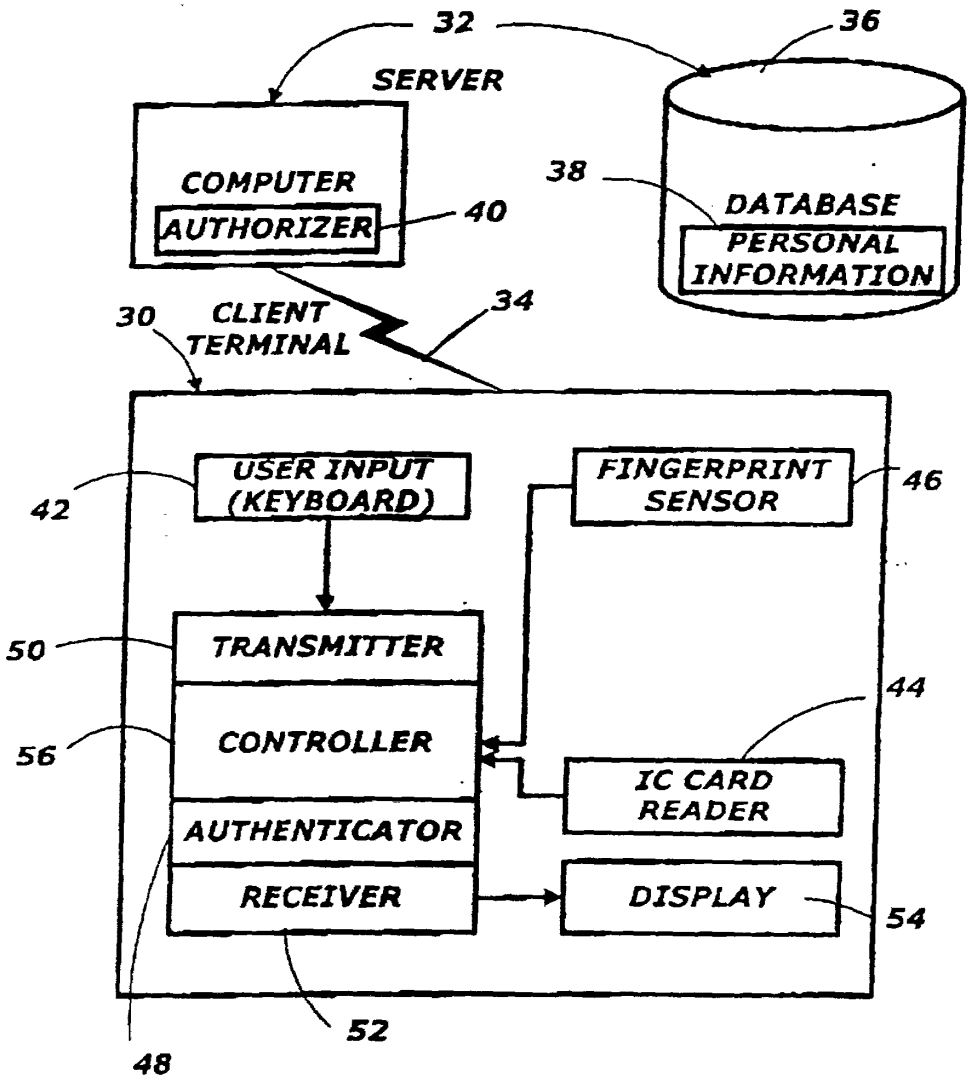
WAVELYNX EX. 1003, Pg. 1645
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG. 1



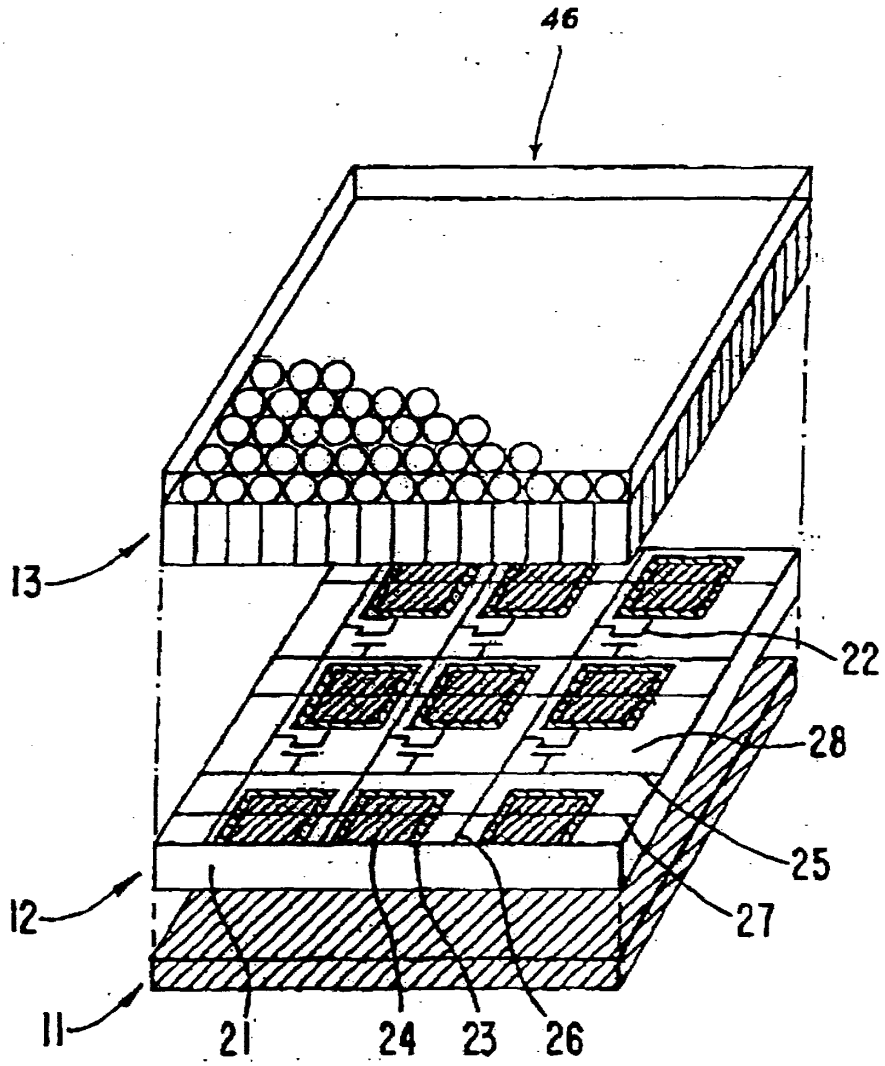
BNSDOCID: <GB___2331825A__I_>

FIG. 2



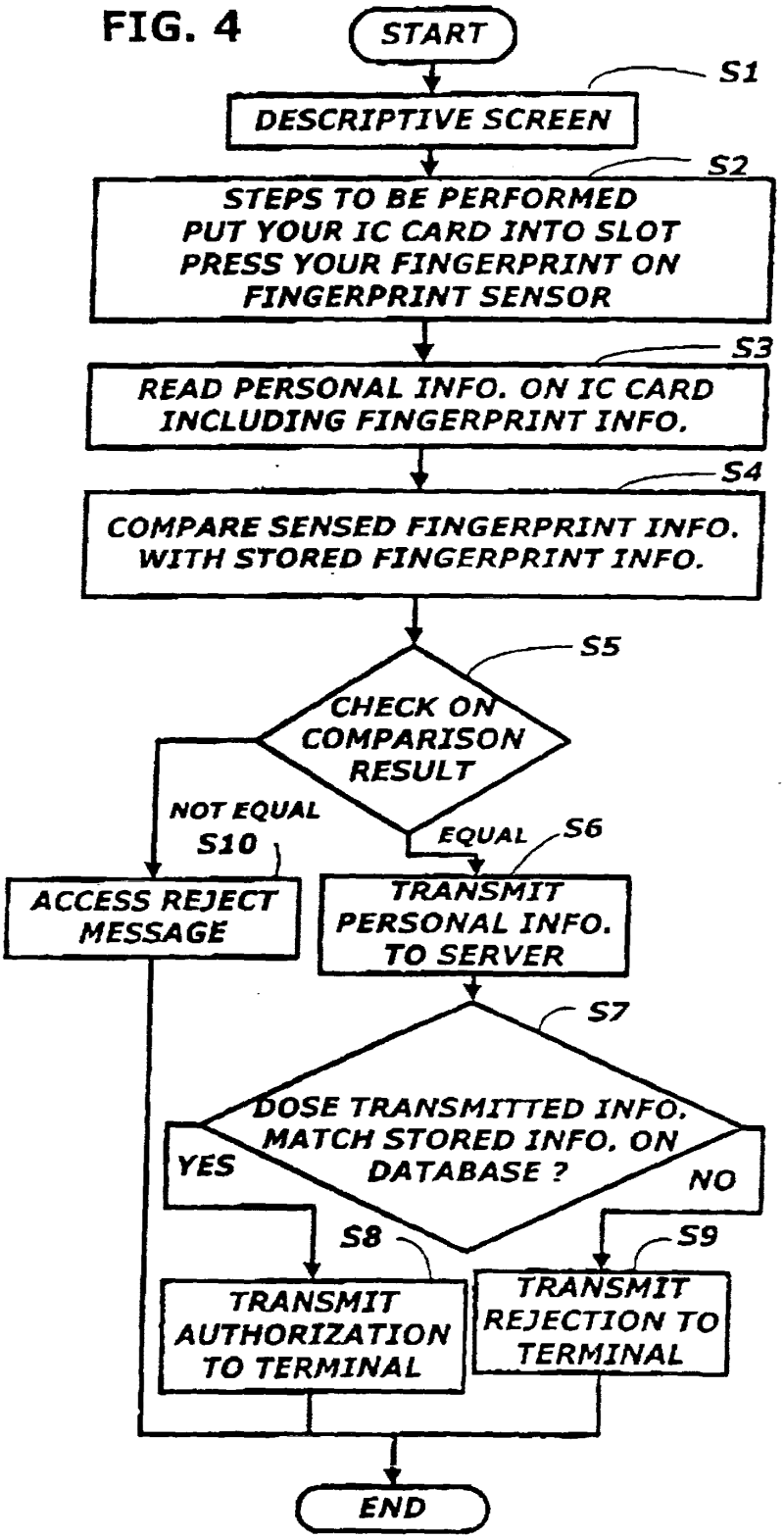
BNSDOCID: <GB___2331825A__I_>

FIG. 3



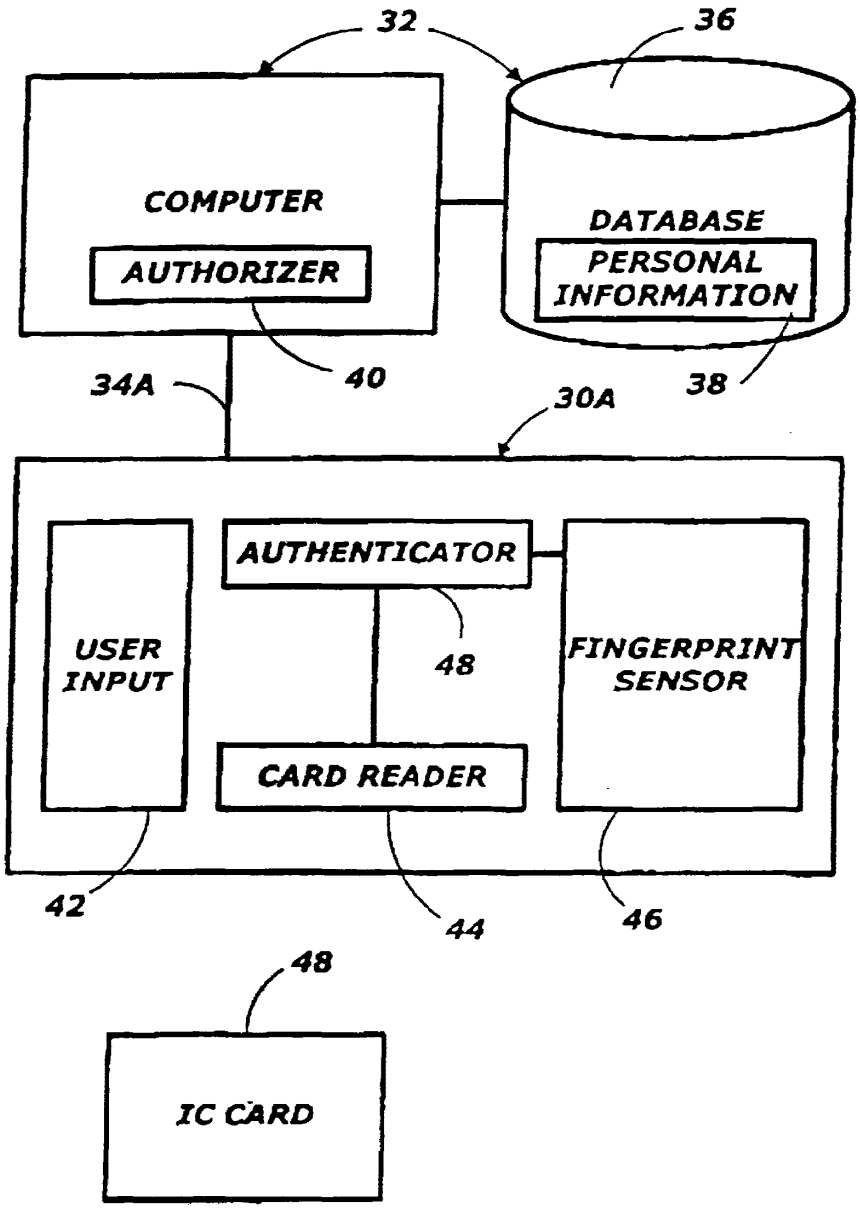
BNSDOCID: <GB___2331825A__I_>

FIG. 4



BNSDOCID: <GB___2331825A__I_>

FIG. 5



BNSDOCID: <GB___2331825A__I_>

Espacenet

Bibliographic data: JP2002261749 (A) — 2002-09-13

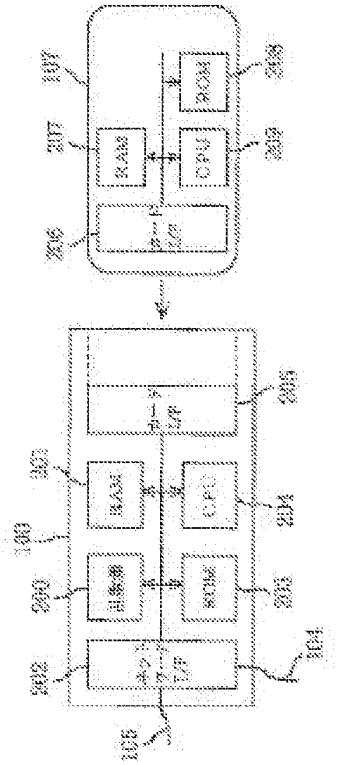
COMMUNICATION SYSTEM

Inventor(s):	KASHIWA HIROSHI ±
Applicant(s):	MATSUSHITA ELECTRIC IND CO LTD ±

Classification:	**- international:**	***G09C1/00; H04L9/10; H04L9/14; H04Q9/00; H04Q9/14;*** (IPC1-7): G09C1/00; H04L9/10; H04L9/14; H04Q9/00; H04Q9/14
	- European:	
Application number:	JP20010051882 20010227	
Priority number (s):	JP20010051882 20010227	

Abstract of JP2002261749 (A)

PROBLEM TO BE SOLVED: To speed up processes, while ensuring a high security, in a communication system for remote-controlling home apparatus over a global network 105. SOLUTION: The system holds unique identification codes, corresponding to a plurality of combinations of encryption algorithms with keys in a home terminal 100 and an IC card 107, in advance. For remote -controlling a home apparatus, it sets the IC card 107 in a public terminal, encrypts control data, using an encryption algorithm and a key corresponding to the identification code and transmits the encryption and the identification code to the home terminal 100, which is then decodes the encryption to generate the control data, using the encryption algorithm and the key corresponding to the received identification code.



WAVELYNX EX. 1003, Pg. 1651
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Last updated: 14.03.2012 Worldwide Database 5.7.38; 92p

WAVELYNX EX. 1003, Pg. 1652
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－261749
（P2002－261749A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.[7]		識別記号	FI			テーマコード(参考)
Ｈ０４Ｌ	9/10		Ｃ０９Ｃ	1/00	６６０Ａ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６６０	Ｈ０４Ｑ	9/00	３０１Ｄ	５Ｋ０４８
Ｈ０４Ｌ	9/14			9/14	Ｈ	
Ｈ０４Ｑ	9/00	３０１	Ｈ０４Ｌ	9/00	６２１Ａ	
	9/14				６４１	

審査請求　未請求　請求項の数４　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－51882(P2001－51882)

(22)出願日　平成13年２月27日(2001.2.27)

(71)出願人　000003821
松下電器産業株式会社
大阪府門真市大字門真1006番地

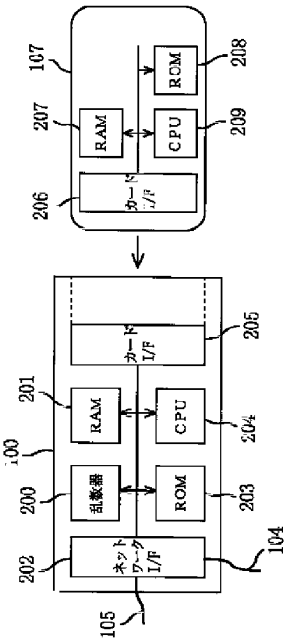
(72)発明者　柏　浩
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　100077931
弁理士　前田　弘　（外７名）

Ｆターム(参考)　5J104 AA01 AA16 EA04 EA26 NA02 NA05 PA15
5K048 AA15 BA12 BA53 DC04 EA13 EA16 HA01 HA02

(54)【発明の名称】　通信システム

(57)【要約】
【課題】　広域ネットワーク１０５を介して家庭用機器を遠隔操作する通信システムで、高い安全性を確保しながら、処理を高速化できるようにする。
【解決手段】　暗号アルゴリズムと鍵との複数の組み合わせに固有の識別コードを対応させ、家庭用端末１００とＩＣカード１０７に保持しておく。家庭用機器を遠隔操作する際に公衆端末にＩＣカード１０７をセットして、識別コードに対応した暗号アルゴリズムと鍵を用いて制御データを暗号化し、暗号と識別コードとを家庭用端末１００に送信する。家庭用端末１００では、受信した識別コードに応じた暗号アルゴリズムと鍵を用いて暗号を復号化し、制御データを生成する。



WAVELYNX EX. 1003, Pg. 1653
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

【特許請求の範囲】
【請求項１】　家庭用端末と外部端末とが接続されたネットワーク上で、外部端末にＩＣカードを接続して家庭用端末側の家庭用機器を遠隔操作する通信システムであって、
家庭用端末とＩＣカードは、それぞれ、複数の鍵と暗号アルゴリズムとを一対一のペアで対応させながら各ペア毎に個別の識別コードを割り当てた同じ内容を記憶する記憶手段を備え、
ＩＣカードは、外部端末にセットされた状態で、前記鍵と暗号アルゴリズムの複数のペアから一つを用いて暗号を生成し、そのペアに対応する識別コードとともにデータを送信する制御手段を備え、
家庭用端末は、外部端末より受信したデータの識別コードから、対応する鍵と暗号アルゴリズムを確定して暗号を復号化する制御手段を備えていることを特徴とする通信システム。
【請求項２】　家庭用端末は、乱数を発生して複数の鍵と識別コードとを生成する乱数発生手段を備え、家庭用端末とＩＣカードは、それぞれ、複数の暗号アルゴリズムを有する暗号アルゴリズム保持手段を備え、
家庭用端末及びＩＣカードの記憶手段は、該家庭用端末にＩＣカードをセットした状態で、一の鍵に一の暗号アルゴリズムと一の識別コードとを対応させながら組み合わせて２以上記憶するように構成されていることを特徴とする請求項１記載の通信システム。
【請求項３】　家庭用端末に複数の家庭用機器が接続されるとともに、家庭用端末とＩＣカードは、鍵と暗号アルゴリズムのペアに対応する識別コードを各家庭用機器毎に割り当てた組み合わせを記憶しており、
ＩＣカードの制御手段は、ＩＣカードが外部端末にセットされた状態で、制御対象となる家庭用機器の識別コードに対応する鍵と暗号アルゴリズムを用いて暗号を生成し、その識別コードとともにデータを送信するように構成され、
家庭用端末の制御手段は、外部端末より受信したデータの識別コードから、対応する鍵と暗号アルゴリズムを確定して暗号を復号化するとともに、制御対象となる家庭用機器を特定するように構成されていることを特徴とする請求項１または２記載の通信システム。
【請求項４】　家庭用端末とＩＣカードの記憶手段は、前記乱数発生手段により発生した値を初期値とするアクセス回数データと、前記アクセス回数データに対して加算または減算するために前記乱数により生成した変更値を記憶しており、
ＩＣカードの制御手段は、ＩＣカードが外部端末にセットされた状態で、前記鍵と暗号アルゴリズムの複数のペアから一つを用いてアクセス回数データを含む暗号を生成し、そのペアに対応する識別コードとともにデータを送信するように構成され、
家庭用端末の制御手段は、外部端末より受信したデータを復号化して、ＩＣカードのアクセス回数データを家庭用端末のアクセス回数データと比較し、両アクセス回数データが一致していると家庭用機器の制御を実行する一方、両アクセス回数データが異なっていると前記ＩＣカード側に前記アクセス回数データの変更を促すように構成され、
さらに、ＩＣカードの制御手段は、前記アクセス回数データを変更した後、その変更前とは異なる識別コードに対応する暗号アルゴリズムと鍵を用いて通信を行うように構成されていることを特徴とする請求項２記載の通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信システムに関し、詳しくは、ＩＣカードを利用して家庭用機器を遠隔操作する通信システムに関するものである。
【０００２】
【従来の技術】近年、広域ネットワークを利用した通信システムに家庭用機器を接続し、任意の端末で個人のＩＣカード（Integrated Circuit Card ）を用いてユーザを認証したうえで、家庭用機器を遠隔で制御・操作できるようにすることが提案されている。このようなシステムで認証を行う技術としては、例えば公開鍵暗号方式による電子署名等が知られている。
【０００３】図１は、ＩＣカードを用いてビデオテープレコーダ（以下、ＶＴＲという）やエアーコンディショナ（エアコン）等の家庭用機器を遠隔制御するための通信システムを示している。この図において、１００は家庭用端末であり、この家庭用端末１００には、ＶＴＲ１０１、エアコン１０２、炊飯器１０３などの家庭用機器が接続され、ローカルエリアネットワーク（ＬＡＮ）１０４が構成されている。
【０００４】一方、家庭用端末１００は、広域ネットワーク１０５を介して公衆端末（外部端末）１０６に接続されている。図には、公衆端末１０６にＩＣカード１０７をセットしようとする状態を示しているが、ＩＣカード１０７は家庭用端末１００にもセットすることができる。
【０００５】次に、このシステム構成において、公開鍵方式によるユーザの認証について説明する。
【０００６】まず、予め家庭用端末１００において、公開鍵Ｐｕと秘密鍵Ｐａを生成し、公開鍵Ｐｕを用いて固有の同期（ＳＹＮＣ）パターンを暗号化（ＳＹＮＣ、Ｐｕ）して、暗号Ａを生成する。そして、この暗号ＡをＩＣカード１０７に記憶しておく。
【０００７】認証時は、ＩＣカード１０７の暗号Ａを公衆端末１０６から家庭用端末１００に広域ネットワーク１０５を介して伝送する。家庭用端末１００では、秘密鍵Ｐａを使って暗号Ａを復号化（暗号Ａ、Ｐａ）し、復

WAVELYNX EX. 1003, Pg. 1654
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

号Ｂを生成する。そして、この復号ＢとＳＹＮＣパターンが一致した場合には認証を成立させて通信を継続し、一致しない場合は認証が不成立であるものとして通信を終了する。

【０００８】

【発明が解決しようとする課題】しかしながら、前記従来の構成では、公開鍵暗号方式の暗号化及び復号化は共通鍵暗号方式に比べて一般に安全性は高いものの、演算量が多いために認証に要する時間が長くなる。また、例えば、素数を用いた公開鍵暗号方式であるＲＳＡ（Rivest,Shamir,Adleman ）暗号方式においては、現在の所は素数を１回で生成及び検証する方法が見つかっていないため、鍵の生成にも時間を要する。そのため、この方式で高速化するためにはパフォーマンスの高いプロセッサが必要であり、高価なシステムになってしまうと言う問題点を有していた。

【０００９】本発明は、このような問題点に鑑みて創案されたものであり、その目的とするところは、ＩＣカードを用いた通信システムにおいて、公開鍵暗号方式を用いなくても高い安全性を確保し、かつパフォーマンスの高いプロセッサを用いなくても処理速度を速くできるようにすることである。

【００１０】

【課題を解決するための手段】本発明は、鍵と暗号アルゴリズムの複数のペアから一つを特定する識別コードをＩＣカードと家庭用端末の間で暗号とともに送受信するようにしたものである。

【００１１】具体的に、本発明が講じた第１の解決手段は、家庭用端末と外部端末とが接続されたネットワーク上で、外部端末にＩＣカードを接続して家庭用端末側の家庭用機器を遠隔操作する通信システムを前提としている。

【００１２】そして、この通信システムでは、家庭用端末とＩＣカードは、それぞれ、複数の鍵と暗号アルゴリズムとを一対一のペアで対応させながら各ペア毎に個別の識別コードを割り当てた同じ内容を記憶する記憶手段を備えている。また、ＩＣカードは、外部端末にセットされた状態で、前記鍵と暗号アルゴリズムの複数のペアから一つを用いて暗号を生成し、そのペアに対応する識別コードとともにデータを送信する制御手段を備え、家庭用端末は、外部端末より受信したデータの識別コードから、対応する鍵と暗号アルゴリズムを確定して暗号を復号化する制御手段を備えている。

【００１３】このように構成すると、ＩＣカードの制御手段は、記憶手段に記憶されている鍵と暗号アルゴリズムのペアの一つにより、前記家庭用機器の制御データなどを暗号化し、外部端末から家庭用端末へ、その暗号を上記ペアに対応する識別コードとともに送信する。また、家庭用端末では、受信した識別コードと記憶手段の内容とから鍵と暗号アルゴリズムを特定し、暗号を復号化する。したがって、復号化された制御データなどに基づいて、家庭用機器の制御を実行できる。

【００１４】また、本発明が講じた第２の解決手段は、上記第１の解決手段において、家庭用端末が、乱数を発生して複数の鍵と識別コードとを生成する乱数発生手段を備え、家庭用端末とＩＣカードが、複数の暗号アルゴリズムを有する暗号アルゴリズム保持手段を備えている。そして、家庭用端末及びＩＣカードの記憶手段は、該家庭用端末にＩＣカードをセットした状態で、一の鍵に一の暗号アルゴリズムと一の識別コードとを対応させながら組み合わせて２以上記憶するように構成されている。

【００１５】第１の解決手段では鍵と暗号アルゴリズムに識別コードを割り当てた内容を予め記憶手段に記憶していてもよいが、第２の解決手段では、複数の鍵と識別コードが乱数により生成され、さらに鍵と暗号アルゴリズムをペアにしながら識別コードを割り当てた内容が、家庭用端末及びＩＣカードの記憶手段に記憶される。この場合、鍵と暗号アルゴリズムを適宜更新することが容易となる。

【００１６】また、本発明が講じた第３の解決手段では、上記第１または第２の解決手段において、家庭用端末に複数の家庭用機器が接続され、家庭用端末とＩＣカードが、鍵と暗号アルゴリズムのペアに対応する識別コードを各家庭用機器毎に割り当てた組み合わせを記憶している。また、ＩＣカードの制御手段は、ＩＣカードが外部端末にセットされた状態で、制御対象となる家庭用機器の識別コードに対応する鍵と暗号アルゴリズムを用いて暗号を生成し、その識別コードとともにデータを送信するように構成され、家庭用端末の制御手段は、外部端末より受信したデータの識別コードから、対応する鍵と暗号アルゴリズムを確定して暗号を復号化するとともに、制御対象となる家庭用機器を特定するように構成されている。

【００１７】このように構成すると、制御対象となる家庭用機器毎に異なる鍵と暗号アルゴリズムを用いて生成された暗号が、対応する識別コードとともに、ＩＣカードと家庭用端末との間で通信される。

【００１８】また、本発明が講じた第４の解決手段は、上記第２の解決手段において、家庭用端末とＩＣカードの記憶手段が、前記乱数発生手段により発生した値を初期値とするアクセス回数データと、前記アクセス回数データに対して加算または減算するために前記乱数により生成した変更値とを記憶している。また、ＩＣカードの制御手段は、ＩＣカードが外部端末にセットされた状態で、前記鍵と暗号アルゴリズムの複数のペアから一つを用いてアクセス回数データを含む暗号を生成し、そのペアに対応する識別コードとともにデータを送信するように構成され、家庭用端末の制御手段は、外部端末より受信したデータを復号化して、ＩＣカードのアクセス回数

WAVELYNX EX. 1003, Pg. 1655
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

データを家庭用端末のアクセス回数データと比較し、両アクセス回数データが一致していると家庭用機器の制御を実行する一方、両アクセス回数データが異なっていると前記ＩＣカード側に前記アクセス回数データの変更を促すように構成されている。さらに、ＩＣカードの制御手段は、前記アクセス回数データを変更した後、その変更前とは異なる識別コードに対応する暗号アルゴリズムと鍵を用いて通信を行うように構成されている。

【００１９】このように構成すると、ＩＣカードと家庭用端末の間で、アクセス回数データの含まれた暗号が識別コードとともに通信され、ＩＣカード側のアクセス回数データと家庭用端末側のアクセス回数データとを比較することで、家庭用機器の制御の可否が判断される。アクセス回数データが一致しないときは、ＩＣカード側のアクセス回数データを更新した後、異なる識別コードに対応した鍵と暗号アルゴリズムにより暗号を再度生成し、通信を行う。

【００２０】

【発明の効果】上記第１，第２の解決手段によれば、識別コードしか公開されないため、高い安全性を確保できる。また、公開鍵方式より処理量が少ない共通鍵暗号方式を用いられるため、パフォーマンスの高い高価なプロセッサを用いなくても、処理速度を速くすることができる。

【００２１】また、上記第３の解決手段によれば、家庭用機器毎に個別の識別コードを使用するようにしているので、仮に１つの家庭用機器に対応する暗号アルゴリズム及び鍵が判明したとしても、他の家庭用機器への影響を少なくすることができる。

【００２２】また、上記第４の解決手段によれば、アクセス回数データを変更したときに、変更前とは異なる識別コードを使用するようにしているので、第３者がアクセス回数データを解析しようとしても困難である。

【００２３】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら説明する。

【００２４】（実施形態１）この実施形態１は、図１に示すように、ＩＣカード１０７を用いてＶＴＲ１０１等の家庭用機器を遠隔制御する通信システムに関するものであり、各端末１００，１０６とＩＣカード１０７とが以下のように構成されている。

【００２５】まず、図２を用いて、家庭用端末１００とＩＣカード１０７の内部構成を説明する。図示するように、家庭用端末１００の内部には、乱数を発生させる乱数発生手段としての乱数器２００、制御データを保持する記憶手段としての不揮発性のランダムアクセスメモリー（ＲＡＭ）２０１、広域ネットワーク１０５とＬＡＮ１０４とを介して通信を行うためのネットワークインターフェース（ネットワークＩ／Ｆ）２０２、家庭用端末１００の制御に必要なプログラムデータと複数の暗号アルゴリズムとを保持する読み込み専用メモリー（ＲＯＭ）２０３、ＲＯＭ２０３のデータに応じて制御を行う制御手段としての中央処理ユニット（ＣＰＵ）２０４、そしてＩＣカード１０７と通信を行うためのカードインターフェース（カードＩ／Ｆ）２０５が設けられており、これらの構成要素２００～２０５が互いに接続されている。

【００２６】前記乱数器２００は、乱数を発生することにより、暗号の生成と復号に必要な鍵と、鍵に対応する固有の識別コードを生成するものとして用いられている。なお、この実施形態では、乱数器２００を用いて乱数を発生するようにしているが、乱数器２００を設ける代わりに、ＲＯＭ２０３の内部のプログラムで乱数を発生するようにしてもよい。

【００２７】前記家庭用端末１００は操作パネル（図示せず）を備えている。この操作パネルは、公衆端末（外部端末）１０６を用いてＶＴＲ１０１等を遠隔操作する際に使用するＩＣカード１０７に、予め必要なデータの書き込みを行うためなどに設けられている。

【００２８】また、ＩＣカード１０７は、その内部に、家庭用端末１００及び公衆端末１０６と通信を行うためのカードＩ／Ｆ２０６、記憶手段としての不揮発性のＲＡＭ２０７、ＩＣカード１０７の制御に必要なプログラムを保持するＲＯＭ２０８、及びＲＯＭ２０８のデータに応じて制御を行う制御手段としてのＣＰＵ２０９を備え、これらの構成要素２０６～２０９が互いに接続されている。ＲＯＭ２０８（またはＲＡＭ２０７）には、家庭用端末１００側と同じ暗号アルゴリズムが記憶されている。

【００２９】このシステムの操作は、以下のように行う。

【００３０】まず、家庭用端末１００側で操作パネルを操作して、暗号アルゴリズム保持手段としてのＲＯＭ２０３に保持されている複数の暗号アルゴリズムの中から一つを選択するとともに、乱数器２００により、暗号に必要な鍵と固有の識別コードを生成する。そして、これを繰り返し、表１に示すように、生成した識別コード及び鍵と、選択された暗号アルゴリズムのプログラムのアドレスとを対応付けるようにしながら、ＲＡＭ２０１に記憶する。

【００３１】

【表１】

WAVELYNX EX. 1003, Pg. 1656
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

識別コード	鍵	アルゴリズム
A	１２３	000～111
B	４５６	222～333
C	７８９	333～444
・ ・	・ ・	・ ・

【００３２】ここで、識別コードは上述したように鍵に対応する固有のコードであり、ＣＰＵ２０４は、複数の鍵を生成する場合に、表１における識別コードに同一の識別コードがないように制御するものとする。

【００３３】次に、ＩＣカード１０７を家庭用端末１００に挿入し、ＩＣカード１０７のカードＩ／Ｆ２０６を家庭用端末１００のカードＩ／Ｆ２０５に接続する。そして、ＲＡＭ２０１に記憶した表１の情報を、家庭用端末１００のカードＩ／Ｆ２０５からＩＣカード１０７のカードＩ／Ｆ２０６を介して、ＣＰＵ２０９の制御によりＲＡＭ２０７に保持する。つまり、表１の情報は、家庭用端末１００にもＩＣカード１０７にも保持される。なお、ＩＣカード１０７は、表１のデータの作成後に家庭用端末１００にセットしてもよいし、表１のデータの作成前に家庭用端末１００にセットしておいてもよい。

【００３４】次に、ＩＣカード１０７を用いて家庭用機器を遠隔操作する際の公衆端末１０６と家庭用端末１００における通信状態について、図３を参照して説明する。図において、公衆端末１０６の３００は家庭用端末１００のアドレス（ここではＩＰアドレスとする）を表すＩＰアドレスデータ、３０１は鍵に対応する固有の識別コード、３０２は暗号データである。この暗号データ３０２は、暗号データ３０２を暗号化する以前のデータが真正なデータであるかどうかを示す情報として用いられるＳＹＮＣパターン３０３と、家庭用機器の制御データ３０４を含んでいる。また、制御データ３０４は、エアコンの制御データ３０５やＶＴＲの制御データ３０６などを含んでいる。

【００３５】一方、家庭用端末１００の３０７は公衆端末１０６のアドレスを示すＩＰアドレスデータ、３０８は識別コード、３０９は暗号データである。また、３１０は、暗号データ３０９を暗号化する前の情報であり、その内容は、公衆端末１０６からのデータの受信完了を示すＡＣＫ情報（受領情報）である。

【００３６】このシステムにおいて、家庭用機器を遠隔操作する場合、まず、個人ＩＣカード１０７を公衆端末１０６に挿入し、セットする。そして、この公衆端末１０６で自宅の家庭用端末１００を操作するために、公衆端末１０６において、家庭用端末１００のＩＰアドレスのデータ３００と、識別コード３０１と、家庭用機器の種類及び内容を含むデータである制御データ３０４を設定する。

【００３７】公衆端末１０６で設定された内容は、ＩＣカード１０７のＲＡＭ２０７に保持される。ＩＣカード１０７のＣＰＵ２０９は、表１に基づいて、設定されたその識別コードに対応した暗号アルゴリズムと鍵をＲＡＭ２０７から特定する。そして、識別コードに対応したアルゴリズムと鍵を用いて、家庭用機器の制御データ３０４に、その制御データ３０４の真正を示す情報としてＲＯＭ２０８に記憶されているＳＹＮＣパターン３０３を付加したものを暗号化して、暗号データ３０２を生成する。さらに、図３の公衆端末側に示すＩＰアドレスデータ３００、識別コード３０１、及び暗号データ３０２からなる所定フォーマットの送信用データを作成して、これを公衆端末１０６のＩＰアドレスデータ３０７と共に、家庭用端末１００に広域ネットワーク１０５を介して送信する。

【００３８】受信した家庭用端末側では、ＣＰＵ２０４が、ＲＡＭ２０１に保持されている表１の内容に照らし合わせ、送られてきた識別コード３０１に応じた暗号アルゴリズムと鍵を確定する。この暗号アルゴリズムと鍵は、公衆端末１０６側で暗号の生成に用いたのと同じものである。そして、この鍵と暗号アルゴリズムとを用いて暗号データ３０２を復号化し、ＳＹＮＣパターン３０３と制御データ３０４を生成する。

【００３９】ここで、家庭用端末１００のＲＯＭ２０３は、制御データ３０４に含まれる機器の種類や制御内容毎に対応するＳＹＮＣパターンを保持している。そして、家庭用端末１００において、復号化したＳＹＮＣパターン３０３と、家庭用端末１００が保持しているＳＹＮＣパターンとを比較する。この比較の結果、両方が一致した場合は、制御データ３０４が真正なデータであるとして、この制御データ３０４による家庭用機器の制御をＣＰＵ２０４がＬＡＮ１０４を介して行う。

【００４０】このようにＳＹＮＣパターンが一致した場合、家庭用端末１００は、ＣＰＵ２０４の制御により、乱数器２００で生成した乱数に基づいて識別コード３０８を生成し、ＲＡＭ２０１に保持されている表１の情報から識別コード３０８に対応した暗号アルゴリズムと鍵を用いて受信完了を示すＡＣＫ情報３１０を暗号化して暗号データ３０９を生成する。そして、受信したＩＰアドレスデータ３０７と、生成した識別コード３０８及び暗号データ３０９とからなる所定フォーマットの受領信号データを作成し、広域ネットワーク１０５を介してこの信号を公衆端末１０６に送信する。

【００４１】この信号を受信した公衆端末１０６では、ＣＰＵ２０９が識別コード３０８に対応する暗号アルゴリズムと鍵をＲＡＭ２０７に保持されている表１の内容より確定し、暗号データ３０９を復号化して、ＡＣＫ情報３１０を確認することで通信を終了する。

【００４２】このようにすることで、鍵や暗号アルゴリ

WAVELYNX EX. 1003, Pg. 1657
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

ズムなどの暗号化に関する情報は配信せずに共通鍵方式による暗号化通信を行うことができ、特に、識別コード、鍵、アルゴリズムを定期的に更新することで、安全性の高い2点間の通信が可能となる。また、公開鍵暗号方式と同等の安全性を確保しながらも、公開鍵方式より演算量が少なくて済むため、パフォーマンスの高いプロセッサを用いなくても処理速度を速くすることが可能となり、システムのコストが高くなることも防止できる。

【００４３】（実施形態２）次に、図４を参照して本発明の実施形態２を説明する。この実施形態２は、実施形態１の通信システムにおいて、制御する家庭用機器毎に個別の識別コードを割り当てるようにしたものである。ここでは、ＶＴＲ１０１とエアコン１０２を制御するものとして説明する。

【００４４】図４は、本実施形態でＩＣカード１０７を用いて家庭用機器１０１，１０２を遠隔操作する際の公衆端末１０６と家庭用端末１００における通信状態を示している。図において、公衆端末１０６の４００は家庭用端末１００のアドレスを表すＩＰアドレスデータ、４０１はＶＴＲ用の識別コードである識別コードＡ、４０２は暗号化したＶＴＲ用制御データ、４０３はエアコン用の識別コードである識別コードＢ、４０４は暗号化したエアコン用制御データである。

【００４５】また、家庭用端末１００の４０５は公衆端末１０６のアドレスを表すＩＰアドレスデータ、４０６はエアコンに関する情報の受信完了を示すＡＣＫ情報、４０７はＶＴＲに関する情報の受信完了を示すＡＣＫ情報である。なお、４０１は公衆端末１０６側で説明したのと同様にエアコン用識別コードＡ、４０３はＶＴＲ用識別コードＢである。

【００４６】本実施形態のシステムでは、実施形態１で説明した表１のデータの作成時に、各識別コード毎に家庭用機器を割り当てるものとする。つまり、各識別コードと鍵と暗号アルゴリズムとを対応させながら、同時に各識別コードに対応する家庭用機器も設定する。そして、このようにして作成した表２のデータを、家庭用端末１００のＲＡＭ２０１とＩＣカード１０７のＲＡＭ２０７に保存する。

【００４７】

【表２】

識別コード	鍵	アルゴリズム	機器
A	２３４	000～111	ＶＴＲ
B	３４５	222～333	エアコン
C	４５６	444～555	炊飯器
・ ・	・ ・	・ ・	・ ・

【００４８】このシステムにおいては、家庭用機器１０１，１０２を公衆端末１０６から遠隔操作する際に、まず、個人ＩＣカード１０７を公衆端末１０６にセットし、この公衆端末１０６において、自宅の家庭用端末１００のＩＰアドレスをＩＰアドレスデータ４００として設定し、かつ、制御しようとする家庭用機器の識別コードと制御データも設定する。

【００４９】ここでは、遠隔制御する家庭用機器はＶＴＲ１０１とエアコン１０２としている。また、前述したように、識別コード及び制御データは、ＶＴＲ１０１用が識別コードＡ４０１及び制御データ４０２で、エアコン１０２用が識別コードＢ４０３及び制御データ４０４とする。

【００５０】公衆端末１０６で設定された内容は、ＩＣカード１０７のＲＡＭ２０７に保持される。そして、ＩＣカード１０７のＣＰＵ２０９は、予め保存された表２の各識別コードに対応した暗号アルゴリズムと鍵をＲＡＭ２０７から確定し、その識別コードに対応したアルゴリズムと鍵を用いて家庭用機器の制御データ４０２と制御データ４０４を暗号化する。そして、図４の公衆端末１０６側に示すように、ＩＰアドレスデータ４００、識別コードＡ４０１、制御データ４０２、識別コードＢ４０３、制御データ４０４からなる所定フォーマットの送信用データを作成し、このデータを公衆端末１０６のＩＰアドレスデータ４０５と共に家庭用端末１００に広域ネットワーク１０５を介して送信する。

【００５１】受信した家庭用端末１００側では、ＣＰＵ２０４がＲＡＭ２０１に保持している表２の内容に照らし合わせ、識別コードＡ４０１と識別コードＢ４０３に応じた暗号アルゴリズムと鍵を確定し、同時に、各識別コードに対応する家庭用機器も確定する。そして、制御データ４０２と制御データ４０４をそれぞれ復号化して元の制御データを生成する。家庭用端末１００のＣＰＵ２０４は、ＬＡＮ１０４を介して制御データ４０２をＶＴＲ１０１に、制御データ４０４をエアコン１０２に転送し、内容に応じた制御を行う。なお、実施形態１と同様、暗号データにＳＹＮＣパターンを含めておき、データが真正であるかどうかを確認するとよい。

【００５２】次に、家庭用端末１００は、ＶＴＲ１０１に関する情報の受信完了を示す情報を識別コードＡ４０１に対応した暗号アルゴリズムと鍵を用いて暗号化してＡＣＫ情報４０６を生成し、同様に、エアコン１０２に

WAVELYNX EX. 1003, Pg. 1658
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

関する情報の受信終了を示す情報を識別コードＢ４０３に対応した暗号アルゴリズムと鍵を用いて暗号化してＡＣＫ情報４０７を生成する。そして、受信したＩＰアドレスデータ４０５と、識別コードＡ４０１、ＡＣＫ情報４０６、識別コードＢ４０３、及びＡＣＫ情報４０７とからなる所定フォーマットの受領信号データを作成し、このデータを広域ネットワーク１０５を介して公衆端末１０６に送信する。

【００５３】受信した公衆端末１０６では、受信した受領信号データに含まれている識別コードＡ４０１と識別コードＢ４０３に応じて、ＣＰＵ２０９が暗号アルゴリズムと鍵をＲＡＭ２０７より確定する。そして、ＡＣＫ情報４０６とＡＣＫ情報４０７を復号化して、このＡＣＫ情報を確認した後、通信を終了する。

【００５４】このように、機器毎に識別コードが異なる設定にすると、仮に１つの家庭用機器の暗号アルゴリズムと鍵が判明しても他の家庭用機器への影響を抑えられ、定期的にＲＡＭ２０１及びＲＡＭ２０７の表２のデータを更新することにより、より安全な通信が可能となる。また、この場合も、従来の公開鍵方式よりも演算量が少なくて済むため、実施形態１と同様にパフォーマンスの高いプロセッサを用いなくても処理速度を速くすることが可能となり、システムのコストが高くなることを防止できる。

【００５５】（実施形態３）次に、図５から図７を参照して本発明の実施形態３を説明する。この実施形態３は、実施形態１の通信システムにおいて、家庭用機器１００と公衆端末１０６との間での認証にアクセス回数データを用いるようにしたものである。

【００５６】図５は、家庭用端末１００のアクセス回数データと、ＩＣカード１０７のアクセス回数データとを用いて行う通信状態を示している。５００はＩＣカード１０７が保持しているアクセス回数データ、５０１はＩＣカード１０７が保持している変更値、５０２は家庭用端末１００が保持しているアクセス回数データ、５０３は家庭用端末１００が保持している変更値である。また、この図５において図３と同一符号は、同一機能を有する情報を示している。

【００５７】このシステムでは、まず、図１，図２の構成において、家庭用端末１００のＣＰＵ２０４が、乱数器２００に２つの乱数を発生させる。そして、一方の乱数をアクセス回数データ５０２とし、もう一方の乱数を変更値５０３としてＲＡＭ２０１に保持し、同様に２つの乱数をカードＩ／Ｆ２０５及びカードＩ／Ｆ２０６を介してＲＡＭ２０７にも保持して、アクセス回数データ５０２に対応する乱数をアクセス回数データ５００とし、変更値５０３に対応する乱数を変更値５０１とする。なお、これらのデータと共に、表１のデータも作成される。

【００５８】家庭用端末１００と公衆端末１０６によるアクセス回数データ５００，５０２を用いた通信は、以下のように行われる。まず、図３の例と同様に公衆端末１０６で識別コード３０１と制御データ３０４を設定すると、図５に示すように、ＳＹＮＣパターン３０３と制御データ３０４に、ＩＣカード１０７に保持しているアクセス回数データ５００を加えたものから、識別コードに対応する鍵と暗号アルゴリズムにより暗号データ３０２が生成される。そして、この暗号データ３０２が、ＩＰアドレスデータ３００及び識別コード３０１とともに家庭用端末１００に転送される。家庭用端末１００は、識別コード３０１から鍵と暗号アルゴリズムとを特定し、暗号データ３０２を復号化する。さらに、受信したＩＣカード１０７のアクセス回数データ５００をＣＰＵ２０４の制御によりＲＡＭ２０１に保持しているアクセス回数データ５０２と比較することで、通信の真正を判断する。

【００５９】図６は、図５でアクセス回数データ５００とアクセス回数データ５０２が一致した場合におけるアクセス回数データ５００，５０２の更新を示す概念図であり、図７は、図５でアクセス回数データ５００とアクセス回数データ５０２が不一致になった場合におけるアクセス回数データ５００，５０２の更新を示す概念図である。

【００６０】図５においてアクセス回数データ５００，５０２が一致した場合には、通信が成立したものとして、家庭用端末１００のＣＰＵ２０４は、家庭用機器を制御するとともに、アクセス回数データ５０２に変更値５０３を加算する。そして、この値を次通信のアクセス回数データ５０２として保持し、公衆端末１０６にＡＣＫ情報を送信する。図６では、アクセス回数データ５０２が「５」であった場合に変更値「３」を加えて「８」に更新し、ＡＣＫ情報を送信する様子を示している。

【００６１】公衆端末１０６は、ＡＣＫ情報が受信されたならば、アクセス回数データ５００に変更値５０１を加算し、その値を次通信のアクセス回数データ５００として保持する。図６では、公衆端末１０６側でもアクセス回数データ５００を「５」から「８」に更新している。

【００６２】一方、図５でアクセス回数データ５００，５０２が不一致になった場合には、通信が成立しなかったものとして、図７に示すように、アクセス回数データ５００，５０２の更新を促す不一致コードを公衆端末１０６に送信する。

【００６３】この不一致コードを受信した公衆端末１０６は、保持しているアクセス回数データ５００に変更値５０１を加算して、その値をアクセス回数データ５００として家庭用端末１００に再度送信する。図では、「５」を「８」に更新して再度送信している。

【００６４】この場合、公衆端末１０６側のＩＣカード１０７のＣＰＵ２０９は、通信スタート時の識別コード

WAVELYNX EX. 1003, Pg. 1659
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

を識別コードAとするならば、家庭用端末１００からアクセス回数データの不一致による変更依頼があったのに対応して公衆端末１０６がアクセス回数データ５００を変更して再送信する場合には、識別コード３０１を前回とは変更して識別コードBを利用するように制御する。

【００６５】家庭用端末１００においても、アクセス回数データの変更を依頼した公衆端末のＩＰアドレスデータとその時の識別コードをＲＡＭ２０１に保持しておき、そのＩＰアドレスからの送信であれば識別コード３０１が変更されているかどうかを確認する。そして、一致すればＡＣＫ情報の送受信とアクセス回数データ５００，５０２の更新とを行って通信を終了し、不一致であれば保持していたＩＰアドレスデータ３００と識別コード３０１を消去して通信を継続する。

【００６６】なお、図６及び図７において、ＡＣＫ情報や不一致コードは、暗号化して識別コードと共に送信するとよい。

【００６７】このようにアクセス回数データ５００，５０２が一致するように制御し、アクセス回数データ５００，５０２が異なる場合に一致させるように、通信する毎に識別コードを異ならせることで、悪意のある者がアクセス回数データ５００，５０２を暴こうとしようとしても通信毎に識別コード３０１が異なることから解析が困難なため、安全性の高い２点間の通信が可能となる。また、この場合も共通鍵暗号方式に比べて演算量が少なくて済むため、パフォーマンスの高いプロセッサを用いなくても処理を高速化できる。

【図面の簡単な説明】

【図１】本発明に係る通信システムが適用されるネットワークの構成図である。

【図２】家庭用端末とＩＣカードの構成図である。

【図３】識別コードを用いたプロトコルの概念図である。

【図４】機器毎に識別コード変更した場合のプロトコルの概念図である。

【図５】アクセス回数データを用いたプロトコルの概念図である。

【図６】図５においてアクセス回数データが一致した場合の通信の概念図である。

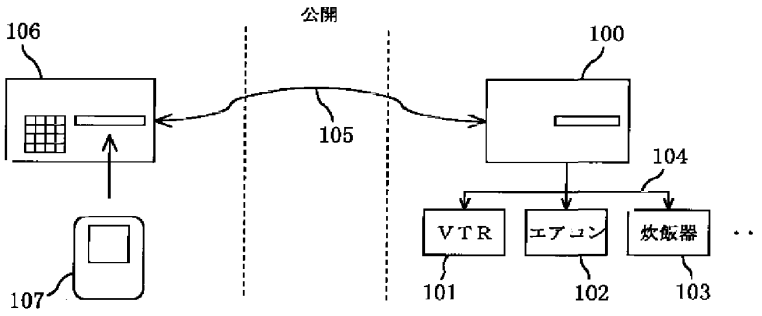
【図７】図５においてアクセス回数データが不一致になった場合の通信の概念図である。

【符号の説明】

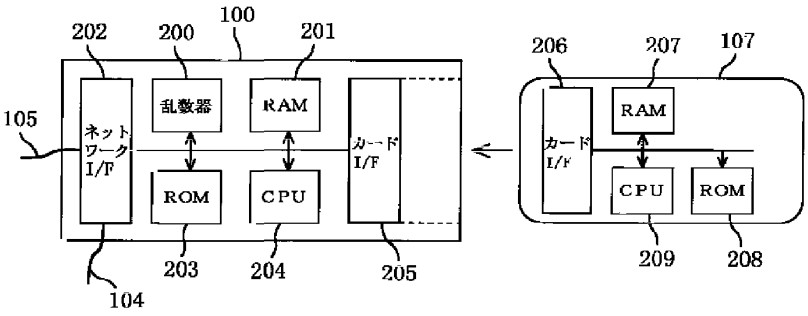
１００　家庭用端末
１０１　ＶＴＲ（家庭用機器）
１０２　エアコン（家庭用機器）
１０３　炊飯器（家庭用機器）
１０４　ＬＡＮ
１０５　広域ネットワーク
１０６　公衆端末（外部端末）
１０７　ＩＣカード
２００　乱数器（乱数発生手段）
２０１　ＲＡＭ（記憶手段）
２０２　ネットワークＩ／Ｆ
２０３　ＲＯＭ（暗号アルゴリズム保持手段）
２０４　ＣＰＵ（制御手段）
２０５　カードＩ／Ｆ
２０６　カードＩ／Ｆ
２０７　ＲＡＭ（記憶手段）
２０８　ＲＯＭ（暗号アルゴリズム保持手段）
２０９　ＣＰＵ（制御手段）
３００　ＩＰアドレスデータ
３０１　識別コード
３０２　暗号データ
３０３　ＳＹＮＣパターン
３０４　制御データ
３０５　エアコン制御データ
３０６　ＶＴＲ制御データ
３０７　ＩＰアドレスデータ
３０８　識別コード
３０９　暗号データ
３１０　ＡＣＫ情報
４００　ＩＰアドレスデータ
４０１　識別コードＡ
４０２　制御データ
４０３　識別コードＢ
４０４　制御データ
４０５　ＩＰアドレスデータ
４０６　ＡＣＫ情報
４０７　ＡＣＫ情報
５００　アクセス回数データ
５０１　変更値
５０２　アクセス回数データ
５０３　変更値

WAVELYNX EX. 1003, Pg. 1660
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

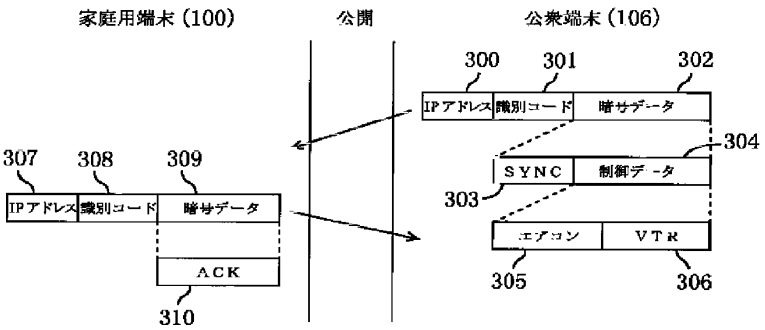
【図１】


公開
106
100
105
104
VTR
エアコン
炊飯器
107
101
102
103

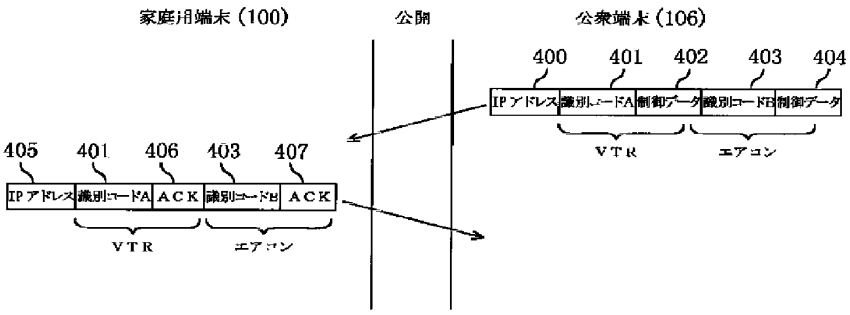
【図２】


100
202
200
201
206
207
107
105
ネットワークI/F
乱数器
RAM
カードI/F
RAM
ROM
CPU
カードI/F
CPU
ROM
203
204
205
209
208
104

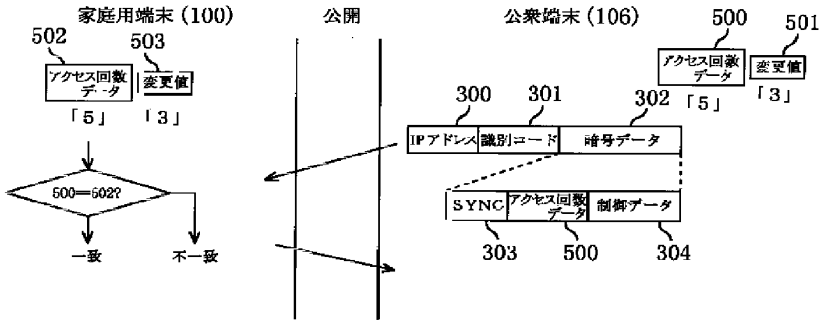
【図３】


家庭用端末 (100)
公開
公衆端末 (106)
300
301
302
IPアドレス
識別コード
暗号データ
304
SYNC
制御データ
303
エアコン
VTR
305
306
307
308
309
IPアドレス
識別コード
暗号データ
ACK
310

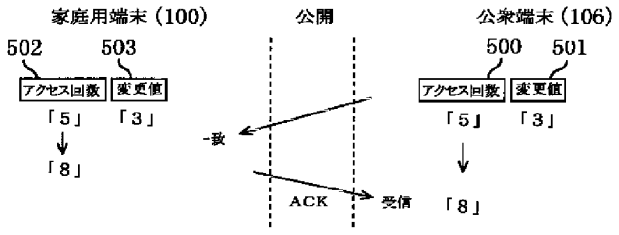
【図4】


家庭用端末(100)
公開
公衆端末(106)
400
401
402
403
404
IPアドレス
識別コードA
制御データ
識別コードB
制御データ
VTR
エアコン
405
401
406
403
407
IPアドレス
識別コードA
ACK
識別コードB
ACK
VTR
エアコン

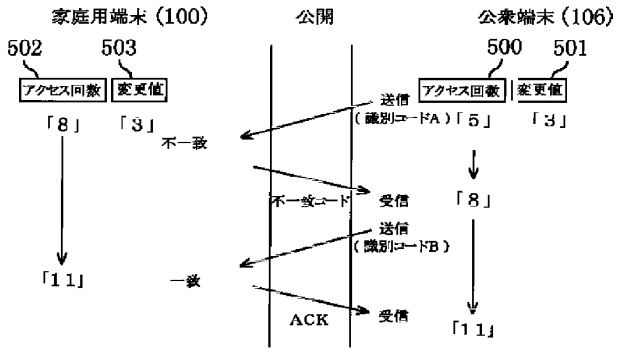
【図5】


家庭用端末(100)
公開
公衆端末(106)
502
503
アクセス回数データ
変更値
「5」
「3」
500=502?
一致
不一致
500
501
アクセス回数データ
変更値
「5」
「3」
300
301
302
IPアドレス
識別コード
暗号データ
SYNC
アクセス回数データ
制御データ
303
500
304

【図6】


家庭用端末(100)
公開
公衆端末(106)
502
503
アクセス回数
変更値
「5」
「3」
「8」
一致
ACK
受信
500
501
アクセス回数
変更値
「5」
「3」
「8」

【図７】


家庭用端末（100）
公開
公衆端末（106）
502
503
500
501
アクセス回数
変更値
アクセス回数
変更値
「８」
「３」
「５」
「３」
送信
（識別コードA）
不一致
不一致コード
受信
「８」
送信
（識別コードB）
「１１」
一致
ACK
受信
「１１」

No active trail

DELPHION

RESEARCH PRODUCTS INSIDE DELPHION

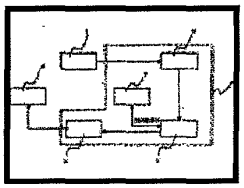
Log Out Work Files Saved Searches My Account Search: Quick/Number Boolean Advanced Derwent

Derwent Record Emai

View: Expand Details Go to: Delphion Integrated View Tools: Add to Work File: Create new Work Fi

Derwent Title: **Serial communication interface for controlling entrance and exit having Wiegand signal automatically generating device and method for managing entrance and exit controlling system using the interface**

Original Title: ☑ KR2073716A: SERIAL COMMUNICATION INTERFACE FOR CONTROLLING ENTRANCE AND EXIT HAVING WIEGAND SIGNAL AUTOMATICALLY GENERATING DEVICE AND METHOD FOR MANAGING ENTRANCE AND EXIT CONTROLLING SYSTEM USING THE INTER



Assignee: **FIRSTECH INT INC** Non-standard company

Inventor: **SUN S G;**

Accession/ Update: **2003-145718 / 200314**

IPC Code: **G06K 19/00 ;**

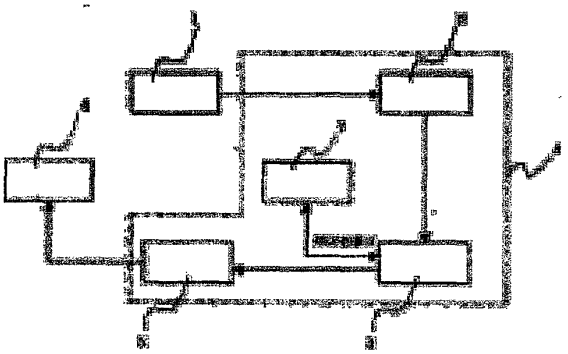
Derwent Classes: T01; T04; T05; U22; V04;

Manual Codes: **T01-C07C1**(Smart card reader interface) , **T01-H01B3A**(Memory card) , **T01-J12C**(Security) , **T04-K02**(Reading and writing aspects) , **T05-D01A** (With card or badge access) , **U22-A02X**(Active element - other) , **V04-Q02A3A**(Contactless cards)

Derwent Abstract: (KR2073716A) **Novelty -** A serial communication interface for controlling an entrance and exit having Wiegand signal automatically generating device and a method for managing an entrance and exit controlling system using the interface are provided to receive a fixed signal being generated in a smart card, generate a Wiegand signal through a Wiegand signal automatically generating device, and transmit the signal to a control unit for controlling an entrance and exit by mounting the Wiegand signal automatically generating device in a serial communication interface for controlling an entrance and exit.

Detailed Description - A smart card(1) stores personal data of a card user and authorized contents to an entrance door. An antenna unit(2) is provided for transmitting all personal signals transmitted in the smart card(1) to a smart card interface module(3). The smart card interface module(3) checks the personal signals received in the antenna unit(2) by a communication with a microprocessor(7) and transmits the signals to a Wiegand signal automatically generating device (5). The Wiegand signal automatically generating device(5) stores an assembler program using a 8-bit CMOS EEPROM micro controller, automatically converts the personal signal into a Wiegand signal, and transmits the signal to an entrance and exit controller(6). The entrance and exit controller(6) searches the transmitted Wiegand signal in data stored in an internal memory and embodies an entrance and exit authority.

Images:



Dwg.1/10

Family:

PDF	Patent	Pub. Date	Derwent Update	Pages	Language	IPC Code
		2002-09-28	200314	1	English	G06K 19/00

WAVELYNX EX. 1003, Pg. 1664
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

KR2073716A *

Local appls.: KR2001000013470 Filed:2001-03-15 (2001KR-0013470)

Priority Number:

Application Number	Filed	Original Title
KR2001000013470	2001-03-15	SERIAL COMMUNICATION INTERFACE FOR CONTROLLING ENTRANCE AND EXIT HAVING WIEGAND SIGNAL AUTOMATICALLY GENERATING DEVICE AND METHOD FOR MANAGING ENTRANCE AND EXIT CONTROLLING SYSTEM USING THE INTER

Pricing Current charges

Derwent Searches: Boolean | Accession/Number | Advanced

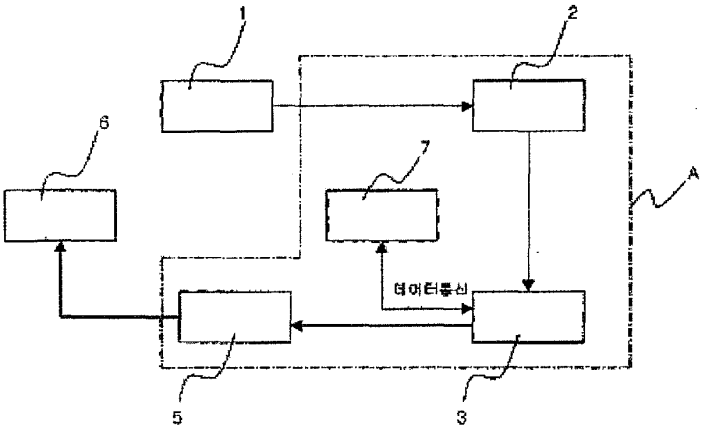
Data copyright Thomson Derwent 2003

THOMSON

Copyright © 1997-2007 The Thoms

Subscriptions | Web Seminars | Privacy | Terms & Conditions | Site Map | Contact Us | Help

WAVELYNX EX. 1003, Pg. 1665
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018



WAVELYNX EX. 1003, Pg. 1666
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
G06K 19/00

(11) 공개번호 특2002- 0073716
(43) 공개일자 2002년09월28일

(21) 출원번호 10- 2001- 0013470
(22) 출원일자 2001년03월15일

(71) 출원인 주식회사 퍼스텍인터내셔날
서울시 서초구 서초동 1569- 15 영진빌딩 3층

(72) 발명자 선상규
경기도용인시수지읍죽전리현대1차아파트103- 104

(74) 대리인 황종환

심사청구 : 있음

(54) 위겐드신호 자동발생장치를 갖춘 출입통제용직렬통신인터페이스 및 그를 이용한 출입통제 시스템의운영방법

요약

본 발명은, 스마트 카드가 카드 인식기에 접근되면 카드 인식기와 카드의 통신을 통해 인증관계를 확인하고, 인증이 확인되면 위겐드(Wiegand) 신호가 자동으로 발생하며, 이렇게 발생된 위겐드신호를 이용하여 기존 RF- 카드 시스템과의 연동을 가능하게 하고, 여러개의 출입문을 중앙제어반에서 동시에 제어할 수 있도록 구성된다.

또한, 스마트 카드는 여러가지의 응용 시스템을 동시에 사용할 수 있는 기능을 가지고 있기 때문에, 출입통제 시스템 뿐만 아니라, 전자지불 및 거래 시스템, 소액 결제 시스템, 본인 인증 시스템, PC 보안 시스템 등과 연계하여 통합시스템으로 구축할 수 있다.

대표도
도 1

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 위겐드신호 자동발생장치가 갖추어진 출입통제용 직렬통신인터페이스의 개략 구성과, 이 출입통제용 직렬통신인터페이스의 위겐드신호 자동발생장치를 이용하여 위겐드신호를 발생시키는 흐름을 나타낸 블록도,

도 2는 본 발명에 따른 위겐드신호 자동발생장치를 갖춘 출입통제용 직렬통신인터페이스를 이용한 출입통제 시스템의 운영방법을 나타낸 시스템 흐름도이다.

WAVELYNX EX. 1003, Pg. 1667
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

〈도면의 주요부분에 대한 부호의 설명〉

1 - - - 스마트 카드,

2 - - - 안테나부,

3 - - - SCI(Serial Communication Interface) : 직렬통신인터페이스,

5 - - - 위겐드신호 자동발생장치,

6 - - - 출입통제 제어기,

7 - - - 마이크로 프로세서,

11 - - - 중앙통제실 영역,

12 - - - 출입통제 제어기 영역,

13 - - - 출입문 영역,

15 - - - 직렬통신인터페이스 영역,

A - - - 스마트 카드 인식부.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 위겐드(Wiegand) 신호 자동발생장치와 출입통제 시스템의 운영방법에 관한 것으로, 특히 출입통제용 직렬통신인터페이스에 위겐드신호 자동발생장치를 장착함으로써, 스마트 카드에서 발생되는 일정한 신호를 수신하여 위겐드신호 자동발생장치를 통해 자동으로 위겐드신호를 발생시켜 출입통제용 제어기로 전송할 수 있는 위겐드신호 자동발생장치를 갖춘 출입통제용 직렬통신인터페이스와, 출입통제 시스템을 하나로 통합할 수 있도록 하는 상기 위겐드신호 자동발생장치를 갖춘 출입통제용 직렬통신인터페이스를 이용한 출입통제 시스템의 운영방법에 관한 것이다.

종래, 일반적으로 사용되는 직렬통신인터페이스(Serial Communication Interface)는 RS-232를 통해 PC와 통신만을 수행할 수 있는 구성으로 되어 있었기 때문에, 중앙에서 여러개의 각 출입문을 동시에 제어할 수 있는 중앙제어식 출입통제 시스템에 적용하기에는 바람직하지 못했다.

또한, 종래의 직렬통신인터페이스는 위겐드신호체계를 갖추고 있지 못하기 때문에, 기존의 스마트 카드를 이용하여 중앙제어식 출입통제 시스템을 구축하기 위해서는 각 개별의 시스템을 각각의 도어(Door)에 구축하면서, 또한 각각의 도어에 구축된 출입통제 시스템을 통합할 수 있는 별도의 시스템을 구축해야만 하므로, 시스템 자체가 너무 복잡해지는 등의 문제가 발생한다.

또한, 종래의 스마트 카드는 출입통제 시스템에 적용할 경우 호환성이 저하되기 때문에, 스마트 카드 단독으로만 사용해야 하는 문제점도 있다.

WAVELYNX EX. 1003, Pg. 1668
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

또한, 종래의 출입통제 시스템의 경우, 단독형과 온- 라인(On- Line) 시스템의 방식이 전혀 다르기 때문에, 시스템간 상호 호환성이 매우 낮다.

따라서, 출입통제 시스템을 교체할 경우에는 시스템 전체를 교체해야만 하는 문제점을 갖게 되는 것이다.

더욱이, 시스템의 운용상에 있어서도, 발생하는 장단점이 서로 대치되기 때문에, 시스템 구축시 적절한 시스템을 선택하는 것이 매우 어렵다는 문제점을 갖고 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기한 점을 감안하여 이루어진 것으로, 출입통제용 직렬통신인터페이스에 위겐드신호 자동발생장치를 장착함으로써, 스마트 카드에서 발생되는 일정한 신호를 수신하여 위겐드신호 자동발생장치를 통해 자동으로 위겐드신호를 발생시켜 출입통제용 제어기로 전송할 수 있는 위겐드신호 자동발생장치를 갖춘 출입통제용 직렬통신인터페이스를 제공하는 것에 그 목적이 있다.

또한, 단독형과 온- 라인 시스템의 구축을 모두 가능하게 하여 호환성을 높이고, 시스템의 확장성을 높여 다른 시스템과의 연계를 가능하게 함으로써 출입통제 시스템을 하나로 통합할 수 있도록 하는 직렬통신인터페이스를 이용한 출입통제 시스템의 운영방법을 제공하는 것에 있다.

발명의 구성 및 작용

상기한 바와 같은 목적을 달성하기 위한 본 발명에 따른 위겐드신호 자동발생장치를 갖춘 출입통제용 직렬통신인터페이스는, 카드 사용자의 개인자료와 출입문에 대한 권한사항이 저장되어 있는 스마트 카드와, 스마트 카드에서 전송된 모든 개별 신호를 스마트 카드 인터페이스 모듈로 전송하기 위한 안테나부, 안테나부에서 전송받은 개별 신호를 마이크로 프로세서와의 통신에 의해 확인한 후, 위겐드신호 자동발생장치로 전송하기 위한 스마트 카드 인터페이스 모듈, 8비트 CMOS EEPROM 마이크로콘트롤러를 이용한 어셈블러 프로그램이 내장되고, 스마트 카드 인터페이스 모듈에서 전송받은 개별 신호를 위겐드신호로 자동변형하여 출입통제 제어기로 전송하기 위한 위겐드신호 자동발생장치 및, 상기의 흐름에 의해 전송된 위겐드신호를 내부 메모리에 저장되어 있는 데이터에서 검색하여 출입권한을 부여하기 위한 출입통제 제어기를 구비하여 구성된 것을 특징으로 한다.

또한, 본 발명에 따른 위겐드신호 자동발생장치를 갖춘 출입통제용 직렬통신인터페이스를 이용한 출입통제 시스템의 운영방법은, 중앙통제실 영역에서 스마트 카드 사용자에 대한 인적사항 및 출입권한 설정에 대한 데이터를 등록하고, 이 등록된 데이터를 전산화 하여 저장하며, 전산화된 데이터를 출입통제 제어기 영역으로 전송하는 단계와, 스마트 카드를 카드 사용자가 카드 인식기 영역의 카드 인식기에 접근시키면, 카드 인식기를 통해 카드의 일련 신호를 인식하여 출입통제 제어기 영역의 제어기가 처리할 수 있는 인식된 카드에 대한 개별 신호를 위겐드신호로 변형하여 출입통제 제어부로 전송하는 단계, 출입통제 제어기 영역에서 상기 중앙통제실 영역의 중앙통제실에서 전송받아 자체 메모리 영역에 저장되어 있는 카드 데이터와 직렬통신인터페이스 영역에서 전송받은 스마트 카드에 대한 위겐드신호를 비교분석하여 출입여부를 판단하는 단계, 출입여부 판단에 따라 출입이 허가된 카드 소지자에 한하여 출입문 개방 명령신호를 출입문 영역에 설치된 전자잠금장치로 전송하게 되고, 허가되지 않은 카드 소지자에 대해서는 개방 명령신호를 출입문 영역으로 전송하지 않으며, 만약 출입문의 강제 개방이나 비정상적인 개방이 발생되면, 출입문 영역에서 전송된 이상 신호를 중앙통제실 영역으로 전송하는 단계 및, 출입문 영역에서 출입통제 제어기 영역으로부터 전송받은 출입문 개방 명령신호에 따라 출입문을 개방하는 단계를 구비하여 이루어진 것을 특징으로 한다.

또한, 본 발명은 중앙통제실 영역에서는 출입통제 및 근태관리 등의 기타 응용 시스템을 운영하고, 카드 사용자가 시스템이 설치된 출입구역을 출입할 때, 이에 대한 관련사항을 화면에 표시하고, 이를 데이터베이스로 구성하여 자체 저장하고, 필요할 때마다 검색할 수 있도록 하는 것을 특징으로 한다.

WAVELYNX EX. 1003, Pg. 1669
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

더욱이, 본 발명은 단독형과 온- 라인 시스템의 구축이 모두 가능하고, 다른 시스템과의 연계가 가능하여 출입통제 시스템을 하나로 통합할 수 있는 것을 특징으로 한다.

(실시예)

이하, 본 발명의 실시예를 도면을 참조하면서 상세히 설명한다.

우선, 도 1을 참조하여 본 발명의 실시예를 상세히 설명한다.

도 1은 본 발명에 따른 위겐드신호 자동발생장치가 갖추어진 출입통제용 직렬통신인터페이스의 개략 구성을 나타내고, 상기 출입통제용 직렬통신인터페이스의 위겐드신호 자동발생장치를 이용하여 위겐드신호를 발생시키는 흐름을 나타낸 블록도이다.

도 1에 도시한 직렬통신인터페이스는, 점선 A로 나타낸 바와 같이 안테나부(2)와, SCI 모듈 및, 위겐드신호 자동발생장치로 구성된다.

도 1에는 위겐드신호의 발생과 전송을 설명하기 위해, 직렬통신인터페이스에 접근시키는 스마트 카드(1) 및 위겐드신호 자동발생장치에서 발생된 신호를 전송받는 출입통제 제어기(6)도 도시하였다.

상기와 같이 구성된 본 발명의 위겐드신호 자동발생장치를 갖춘 스마트 카드의 구성을 보다 구체적으로 설명한다.

카드 사용자의 개인자료와 출입문에 대한 권한사항이 저장되어 있는 스마트 카드(1)를 카드 사용자가 직렬통신인터페이스에 인식시켜, 카드의 모든 개별 신호를 전송한다.

다음에, 안테나부(2)는 스마트 카드(1)에서 전송된 모든 개별 신호를 스마트 카드 인터페이스 모듈(3)로 전송한다.

다음에, 상기 안테나부(2)에서 전송받은 개별 신호를 스마트 카드 인터페이스 모듈(3)은 마이크로 프로세서(7)와의 통신에 의해 확인한 후, 위겐드신호 자동발생장치(5)로 전송한다.

다음에, 8비트 CMOS EEPROM 마이크로콘트롤러를 이용한 어셈블러 프로그램이 내장된 위겐드신호 자동발생장치(5)는 스마트 카드 인터페이스 모듈(3)에서 전송받은 개별 신호를 위겐드신호로 자동변형하여 출입통제 제어기(6)로 전송하게 된다.

최종적으로, 상기의 흐름에 의해 전송된 위겐드신호를 출입통제 제어기(6)에 저장되어 있는 데이터에서 검색하여 출입권한을 부여하게 되는 것이다.

이상 기술한 바와 같이, 도 1은 위겐드신호 발생과정을 나타낸 것으로, 개인의 신상자료와 출입구역에 대한 등급 등이 저장된 스마트 카드와, 이러한 카드를 인식할 수 있는 출입통제용 직렬통신인터페이스 및, 출입통제의 권한을 부여할 수 있는 출입통제 제어기로 구성된 것이다.

이하, 도 2를 참조하여 본 발명에 따른 출입통제 시스템을 하나로 통합할 수 있도록 하는 상기 위겐드신호 자동발생장치를 갖춘 출입통제용 직렬통신인터페이스를 이용한 출입통제 시스템의 운영방법을 설명한다.

도 2는 위겐드신호 자동발생장치를 갖춘 출입통제용 직렬통신인터페이스를 이용한 출입통제 시스템의 운영방법을 나타낸 시스템 흐름도이다.

우선, 도 2에 도시한 바와 같이, 중앙통제실 영역(11)에서는 스마트 카드(1) 사용자에 대한 인적사항 및 출입권한 설정에 대한 데이터를 등록하고, 이 등록된 데이터를 전산화 하여 저장하며, 전산화된 데이터를 출입통제 제어기 영역(12)으로 전송하여 저장시킨다.

WAVELYNX EX. 1003, Pg. 1670
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

또한, 중앙통제실 영역(11)에서는 출입통제 및 근태관리 등의 기타 응용 시스템을 운영하고, 카드 사용자가 시스템이 설치된 출입구역을 출입할 때, 이에 대한 관련사항을 화면에 표시하고, 이를 데이터베이스로 구성하여 자체 저장하고, 필요할 때마다 검색할 수 있도록 한다.

이와 관련하여, 내부의 마이크로칩에 카드 사용자의 개인자료와 출입구역에 대한 등급 등이 저장되어 있는 스마트 카드(1)를 카드 사용자가 카드 인식기 영역(11)의 카드 인식기에 접근시키면, 카드 인식기를 통해 카드의 일련 신호를 인식하여 출입통제 제어기 영역(12)의 제어기가 처리할 수 있는 인식된 카드에 대한 개별 신호를 위겐드신호로 변형하여 출입통제 제어부로 전송한다.

그러면, 출입통제 제어기 영역(12)에서는 상기 중앙통제실 영역(11)의 중앙통제실에서 전송받아 자체 메모리 영역에 저장되어 있는 카드 데이터와 직렬통신인터페이스 영역(15)에서 전송받은 스마트 카드(1)에 대한 위겐드신호를 비교 분석하여 출입여부를 판단한다.

이 경우, 상기 출입여부 판단에 따라 출입이 허가된 카드 소지자에 한하여 출입문 개방 명령신호를 출입문 영역(13)에 설치된 전자잠금장치로 전송하게 되고, 허가되지 않은 카드 소지자에 대해서는 개방 명령신호를 출입문 영역(13)으로 전송하지 않으며, 만약 출입문의 강제 개방이나 비정상적인 개방이 발생되면, 출입문 영역(13)에서 전송된 이상 신호를 중앙통제실 영역(11)으로 전송한다. 이러한 일련의 과정을 중앙통제실로 RS- 232방식으로 전송한다.

최종적으로, 출입자의 무단출입을 방지하기 위해 전자잠금장치가 설치된 출입문 영역(13)에서는 출입통제 제어기 영역(12)에서 전송받은 출입문 개방 명령신호에 따라 출입문을 개방하게 된다.

더욱이, 상기 카드 인식기는 8개의 도어를 장착할 수 있으며, 출입통제 제어기는 128개의 제어기를 연동시킬 수 있다.

발명의 효과

이상 설명한 바와 같이 본 발명은, 출입통제용 스마트 카드 시스템을 적용하게 되면, 스마트 카드의 여러기능을 하나의 시스템으로 통합할 수 있으며, 이러한 시스템 통합에 의해 시스템의 관리를 효과적이고 합리적으로 수행할 수 있다.

또한, 외부의 다른 시스템과도 연계가 가능하여, 버스카드, 전철카드, 신용결제카드 등의 전자화폐와도 통합 시스템 구축의 확장이 가능하다.

더욱이, 출입통제용 직렬통신인터페이스를 적용하게 되면, 기존에 구축되어 있는 RF- 카드를 이용한 출입통제 시스템을 스마트 카드를 이용한 시스템으로 교체할 경우, 출입통제용 직렬통신인터페이스와 카드만을 교체하면 기존의 시스템과도 사용이 가능하기 때문에, 구축비용이 절감되고, 향후 다른 시스템과의 통합시스템 구축에도 효과적이다.

(57) 청구의 범위

청구항 1.

카드 사용자의 개인자료와 출입문에 대한 권한사항이 저장되어 있는 스마트 카드(1)와,

상기 스마트 카드(1)에서 전송된 모든 개별 신호를 스마트 카드 인터페이스 모듈(3)로 전송하기 위한 안테나부(2),

상기 안테나부(2)에서 전송받은 개별 신호를 마이크로 프로세서(7)와의 통신에 의해 확인한 후, 위겐드신호 자동발생장치(5)로 전송하기 위한 스마트 카드 인터페이스 모듈(3),

8비트 CMOS EEPROM 마이크로콘트롤러를 이용한 어셈블러 프로그램이 내장되고, 스마트 카드 인터페이스 모듈(3)에서 전송받은 개별 신호를 위겐드신호로 자동변형하여 출입통제 제어기(6)로 전송하기 위한 위겐드신호 자동발생장치(5) 및,

WAVELYNX EX. 1003, Pg. 1671
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

상기의 흐름에 의해 전송된 위겐드신호를 내부 메모리에 저장되어 있는 데이터에서 검색하여 출입권한을 부여하기 위한 출입통제 제어기(6)를 구비하여 구성된 것을 특징으로 하는 위겐드신호 자동발생장치를 갖춘 출입통제용 직렬통신 인터페이스.

청구항 2.

위겐드신호 자동발생장치를 갖춘 출입통제용 직렬통신인터페이스를 이용한 출입통제 시스템의 운영방법에 있어서,

중앙통제실 영역(11)에서 스마트 카드(1) 사용자에 대한 인적사항 및 출입권한 설정에 대한 데이터를 등록하고, 이 등록된 데이터를 전산화 하여 저장하며, 전산화된 데이터를 출입통제 제어기 영역(12)으로 전송하는 단계와,

상기 스마트 카드(1)를 카드 사용자가 카드 인식기 영역(11)의 카드 인식기에 접근시키면, 카드 인식기를 통해 카드의 일련 신호를 인식하여 출입통제 제어기 영역(12)의 제어기가 처리할 수 있는 인식된 카드에 대한 개별 신호를 위겐드 신호로 변형하여 출입통제 제어부로 전송하는 단계,

상기 출입통제 제어기 영역(12)에서 상기 중앙통제실 영역(11)의 중앙통제실에서 전송받아 자체 메모리 영역에 저장되어 있는 카드 데이터와 직렬통신인터페이스 영역(15)에서 전송받은 스마트 카드(1)에 대한 위겐드신호를 비교분석하여 출입여부를 판단하는 단계,

상기 출입여부 판단에 따라 출입이 허가된 카드 소지자에 한하여 출입문 개방 명령신호를 출입문 영역(13)에 설치된 전자잠금장치로 전송하게 되고, 허가되지 않은 카드 소지자에 대해서는 개방 명령신호를 출입문 영역(13)으로 전송하지 않으며, 만약 출입문의 강제 개방이나 비정상적인 개방이 발생되면, 출입문 영역(13)에서 전송된 이상 신호를 중앙통제실 영역(11)으로 전송하는 단계 및,

상기 출입문 영역(13)에서 출입통제 제어기 영역(12)으로부터 전송받은 출입문 개방 명령신호에 따라 출입문을 개방하는 단계를 구비하여 이루어진 것을 특징으로 하는 출입통제 시스템의 운영방법.

청구항 3.

제2항에 있어서, 상기 중앙통제실 영역(11)에서는 출입통제 및 근태관리 등의 기타 응용 시스템을 운영하고, 카드 사용자가 시스템이 설치된 출입구역을 출입할 때, 이에 대한 관련사항을 화면에 표시하고, 이를 데이터베이스로 구성하여 자체 저장하고, 필요할 때마다 검색할 수 있도록 하는 것을 특징으로 하는 출입통제 시스템의 운영방법.

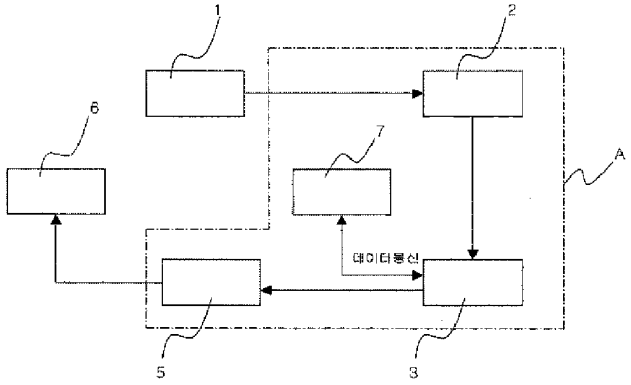
청구항 4.

제2항에 있어서, 상기 시스템 운영방법은 단독형과 온- 라인 시스템의 구축이 모두 가능하고, 다른 시스템과의 연계가 가능하여 출입통제 시스템을 하나로 통합할 수 있는 것을 특징으로 하는 출입통제 시스템의 운영방법.

WAVELYNX EX. 1003, Pg. 1672
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

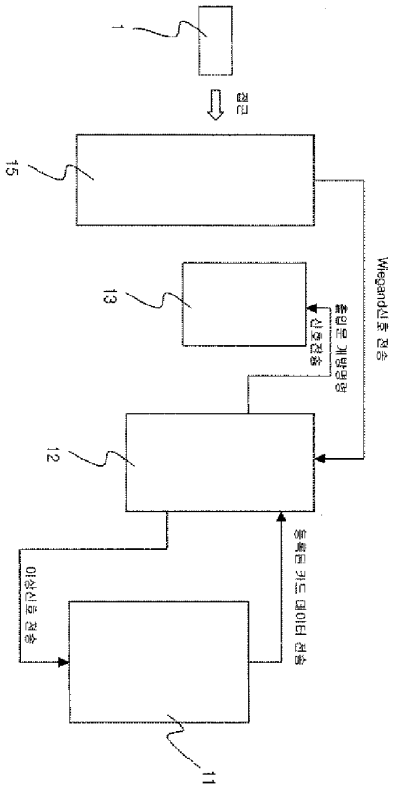
도면

도면 1



WAVELYNX EX. 1003, Pg. 1673
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

도면 2



WAVELYNX EX. 1003, Pg. 1674
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Espacenet

Bibliographic data: RU2158444 (C2) — 2000-10-27

ELECTRONIC MONITORING SYSTEM/NETWORK

Inventor(s): LUSMOR N BERT [US]; EHRMAN KENNET [US]; DZHEHGID BRJUS [US] ± (LUSMOR N. BERT, ; EHRMAN KENNET, ; DZHEHGID BRJUS)

Applicant(s): AJ DI SISTEMS INK [US] ± (AJ DI SISTEMS, INK)

Classification: **- international:** ***G08B13/14;*** (IPC1-7): G08B13/14
- Euro:

Application number: RU19980110566 19951106

Priority number (s): RU19980110566 19951106

Abstract of RU2158444 (C2)

computer engineering. SUBSTANCE: network system of programmed node in fixed position and mobile labeling nodes provides direct communication between nodes. Specific nodes are programmed for recognition of extreme conditions in environment and logical actions using other parameters of conditions under recognition, as well communication to other nodes. Each node has integral circuit, which has three autonomous processors, which have shared memory and control circuit, but use separate registers. First processor provides monitoring of access to units, and has receiving- transmitting units for receiving and transmitting information. Second processor starts code, which is stored for specific usage layer, as well as complete operating system, which is equipped with direct communication to input-output devices for preliminary processing using conditions in environment. Third processor connects application processor to communication processor and controls various operations in the network: data processing, addressing, and so on. Node set is designed as global network, which has autonomous control. EFFECT: increased functional capabilities. 43 cl, 3 dwg, 5 ex

Last updated: 24.09.2012 Worldwide Database 5.7.44.2; 92p

WAVELYNX EX. 1003, Pg. 1675
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) **RU** (11) **2 158 444** (13) **C2**

(51) МПК[7] **G 08 B 13/14**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 98110566/09, 06.11.1995

(24) Дата начала действия патента: 06.11.1995

(46) Дата публикации: 27.10.2000

(56) Ссылки: US 5266925 A, 30.11.1993. RU 2020590 C1, 30.09.1994. RU 2025780 C1, 30.12.1994. US 4656463 A, 07.04.1987. US 5426425 A, 20.06.1995.

(85) Дата перевода заявки PCT на национальную фазу: 08.06.1998

(86) Заявка PCT:
US 95/14376 (06.11.1995)

(87) Публикация PCT:
WO 97/17683 (15.05.1997)

(98) Адрес для переписки:
103062, Москва, ул. Покровка, д.27, строение 1 АГ, Кооперативное агенство интеллектуальной собственности "ИНТЭЛС", Дьяконовой О.М.

(71) Заявитель:
АЙ ДИ СИСТЕМС, ИНК. (US)

(72) Изобретатель: ЛУСМОР Н. Берт (US), ЭРМАН Кеннет (US), ДЖЭГИД Брюс (US)

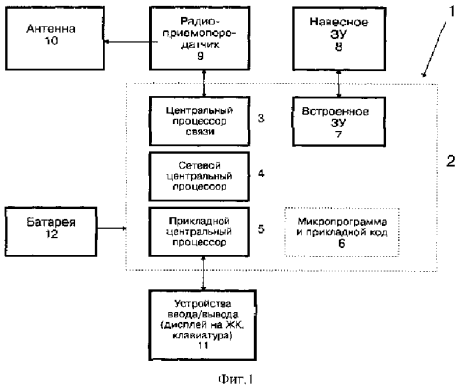
(73) Патентообладатель:
АЙ ДИ СИСТЕМС, ИНК. (US)

RU 2158444 C2

(54) ЭЛЕКТРОННАЯ КОНТРОЛИРУЮЩАЯ СИСТЕМА/СЕТЬ

(57)

Сетевая система программируемых узлов в фиксированной позиции и передвижных узлов бирок обеспечивает прямое сообщение между узлами. Отдельные узлы запрограммированы на распознавание экстремальных условий окружения и логические действия на основе параметров распознанных условий, а также сообщение с другими узлами. Каждый из узлов включает интегральную схему, имеющую три автономных процессора, которые имеют общую память и контрольную схему, но отдельные работы регистров. Первый процессор обеспечивает контроль доступа к средствам и сообщение между узлами и включает приемопередающие элементы для приема и передачи информации. Второй процессор запускает код, записанный для конкретного слоя использования, а также всю операционную систему, которая оснащена прямой связью с устройством ввода/вывода для первоначальной обработки на основе окружающих условий. Третий процессор связывает прикладной процессор со связным процессором и управляет различными операциями в сети - обработкой данных, адресацией и т.п. Узлы формируют автономно управляемую всеобщую сеть, что и является достигаемым техническим результатом. 3 с. и 40 з.п.ф-лы, 3 ил.



Фиг.1

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1676
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) **RU** (11) **2 158 444** (13) **C2**

(51) Int. Cl.[7] **G 08 B 13/14**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **98110566/09, 06.11.1995**

(24) Effective date for property rights: **06.11.1995**

(46) Date of publication: **27.10.2000**

(85) Commencement of national phase: **08.06.1998**

(86) PCT application:
US 95/14376 (06.11.1995)

(87) PCT publication:
WO 97/17683 (15.05.1997)

(98) Mail address:
103062, Moskva, ul. Pokrovka, d.27, stroenie 1 AG, Kooperativnoe agenstvo intellektual'noj sobstvennosti "INTEhLS", D'jakonovoj O.M.

(71) Applicant:
AJ DI SISTEMS, INK. (US)

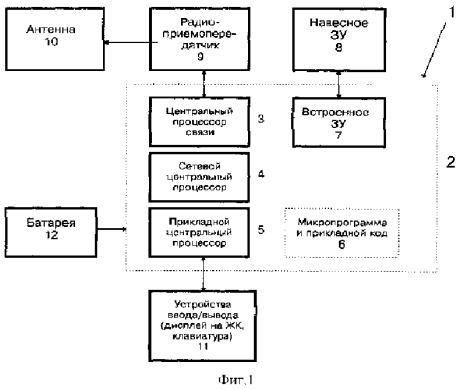
(72) Inventor: **LUSMOR N. Bert (US), EhRMAN Kennet (US), DZhEhGID Brjus (US)**

(73) Proprietor:
AJ DI SISTEMS, INK. (US)

(54) ELECTRONIC MONITORING SYSTEM/NETWORK

(57) Abstract:

FIELD: computer engineering. SUBSTANCE: network system of programmed node in fixed position and mobile labeling nodes provides direct communication between nodes. Specific nodes are programmed for recognition of extreme conditions in environment and logical actions using other parameters of conditions under recognition, as well communication to other nodes. Each node has integral circuit, which has three autonomous processors, which have shared memory and control circuit, but use separate registers. First processor provides monitoring of access to units, and has receiving-transmitting units for receiving and transmitting information. Second processor starts code, which is stored for specific usage layer, as well as complete operating system, which is equipped with direct communication to input-output devices for preliminary processing using conditions in environment. Third processor connects application processor to communication processor and controls various operations in the network: data processing, addressing, and so on. Node set is designed as global network, which has autonomous control. EFFECT: increased functional capabilities. 43 cl, 3 dwg, 5 ex



Фиг.1

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1677
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Данное изобретение относится к системам распознавания и определения местоположения объекта или человека, в частности к системам, которые используются для слежения за персоналом и материальными ценностями.

УРОВЕНЬ ТЕХНИКИ

Хотя для распознавания и определения местоположения объектов и людей было разработано и запатентовано много систем, эти системы позволяют лишь считывать данные с идентификационной бирки (прим. ред.: tag - тэг, идентификационный признак, бирка, маркер) или программировать данные в бирке (режим считывания-записи) и делали это только по запросу. Кроме того, почти все эти системы требуют использования централизованной базы данных или централизованного процессора. Примерами таких систем могут служить электронная система распознавания (4,937,581 и 5,132,687) и переносной определяющий микропроцессор, программируемый пользователем (5,218,343). Были разработаны и другие способы распознавания с описанием протокола, а значит и способа распознавания бирок, например электронный способ запроса бирки распознавания (5,266,925). Все эти бирки по сути имеют устройства накопления памяти с ограниченной чувствительностью. Из-за внешних условий они не могут автономно действовать или воздействовать каким-нибудь способом логического восприятия. Кроме того, даже в сетевых антеннах не существует интерактивного распределения информации между бирками или системного принятия решений, кроме как через центральный процессор.

Задачей данного изобретения является обеспечение сети программируемых узлов, каждый из которых имеет возможность реагировать на заранее запрограммированные специфические внешние условия и сообщаться с другими элементами в сети, посылая сообщения без запроса, запрашивая информацию или давая сигнал тревоги при определенных условиях.

Задачей данного изобретения также является оснащение каждого узла в сети микропроцессором и микропрограммами, которые обеспечивают узлу возможность принимать решения независимо от центрального процессора.

Еще одной задачей данного изобретения является использование способности каждого узла принимать решения для определения соответствующего расстояния для каждой передачи в соответствии с контекстом сообщения.

Еще одной задачей данного изобретения является использование сети для слежения за объектами и определения их местоположения, включая распознавание в различных приложениях.

И еще одной задачей данного изобретения является обеспечение сети для контроля различных параметров, включая внешние условия.

Эта и другие задачи, особенности и преимущества данного изобретения станут более понятными из нижеследующего обсуждения и фигур, на которых:

КРАТКОЕ ОПИСАНИЕ ФИГУР

Фигура 1 - блок-схема, представляющая компоненты узла;

фигура 2 - блок- схема, представляющая компоненты узла фиксированного положения;

фигура 3 - схема размещения бирки и узлов фиксированной позиции (FPN) для слежения за объектами и людьми, а также распознавания, определения местоположения и иного рода оценки подобной информации.

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

В целом данное изобретение включает способ определения местоположения и распознавания объектов и людей, слежения за ними и за параметрами, относящимися к системе в условиях определенных ситуаций, а также способ контроля таких ситуаций. Данное изобретение также включает автономную систему контроля и оценки параметров, а также контрольную систему определения местоположения и распознавания, включающую не менее двух активных операционных узлов, подвижный узел бирки распознавания и обработки данных или как минимум один программируемый узел фиксированной позиции (FPN). FPN находятся в известных фиксированных позициях, а узлы бирок по отношению к ним являются подвижными. Отношение между фиксированными и подвижными узлами (т.е., близость подвижного узла бирки относительно одного или нескольких фиксированных узлов) обеспечивает функцию определения местоположения. Все узлы первоначально оснащены распознавательным кодом, который определяет, где какой узел устанавливается и за кем или чем ведется контроль. Подвижный узел бирки также в случае необходимости программируется для контроля, сохранения, изменения и/или обработки внешних условий путем изменения положений.

Каждый из узлов включает средства непосредственного межузлового сообщения и средства, позволяющие принимать решения без центрального процессора. Узлы бирок также включают средства быстрого сообщения с другими узлами бирок или FPN через радиосвязь.

Отдельные узлы (как подвижные, так и фиксированные) включают встроенный источник питания, такой как долгосрочная батарейка - для подвижных узлов, и непосредственно подсоединенный постоянный источник питания - для фиксированных узлов. Узлы также включают микропроцессор и элементы памяти, при необходимости предварительно запрограммированные, для распознавания внешних условий и запросов и для логических действий на основе распознанных параметров условий (полученных через средства ввода-вывода), а также средства для сообщения с другими узлами для приведения в действие всей сети или ее части, например, через приемопередающие средства (средства дуплексной связи). Расстояние для сообщения через дуплексную радиосвязь определяется микропроцессорными средствами и зависит от передаваемого сообщения. Информация о внешних условиях поступает через запрос по радиосвязи из других узлов, а также присоединенных устройств ввода-вывода.

Каждый из узлов бирки и FPN имеет свой уникальный идентификационный номер,

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1678
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

которым он адресуется и идентифицируется. Каждый узел включает функционально контролируемую им интегральную схему, в оптимальном варианте имеющую как минимум три автономных микропроцессора, которые обладают общей схемой памяти и контроля, однако каждый имеет отдельный комплект регистров.

В интегральной схеме в оптимальном варианте первый микропроцессор или центральный процессор связи обеспечивает контроль доступа к средствам и включает соединение с приемопередающими средствами для получения и передачи информации между узлами (например, между биркой и FPN, между бирками (тэгами) или от FPN к FPN).

Второй микропроцессор представляет собой прикладной центральный процессор, который запускает код, записанный для использования конкретным узлом. Этот второй микропроцессор имеет прямую связь с устройством ввода-вывода для первоначальной обработки на основе внешних условий, как заранее запрограммировано, а также для вмешательства человека для ввода и получения информации. Вводить данные можно, например, при помощи клавиатуры, датчиков условий, таких как термометр и т.п. Примерами устройств вывода могут служить жидкокристаллический дисплей, звуковой сигнал и т.п.

Третий микропроцессор, сетевой центральный процессор, связывает прикладной центральный процессор с центральным процессором связи и управляет обработкой сетевых переменных, адресацией, диалоговой обработкой запросов, аутентификацией, координацией работы сети и т.п.

Микропроцессоры с дополнительной цифровой схемой, средствами связи и ввода-вывода, с конкретной конфигурацией и источником питания обеспечивают компоненты автономно управляемой сети на определенном участке, способные к распознаванию местонахождения, слежению и логическому контролю запрограммированных внешних условий и логическому взаимодействию с внешними запросами для операций по диалоговой обработке. Один из характерных случаев применения - определение местоположения служащего на рабочем месте. Среди других примеров применения - определение местоположения врачей и оборудования в пределах больницы, слежение за пациентом, определение местоположения продуктов и инвентаря, а также слежение за продукцией на складах или в производственных помещениях, автоматический хронометраж и изучение трудовых движений, слежение за транспортированием грузов и т.п., а также - при охране учебных зданий, жилых и прочих зданий от нежелательных посетителей, а также контроль температурных условий при хранении скоропортящихся товаров.

Отдельные узлы обеспечивают функцию интеллектуальной обработки. Например, при определении местоположения персонала с контролем безопасности в узлах бирок запрограммированы параметры уровня безопасности, что позволяет системе должным образом определять местоположение бирок и их носителей. Кроме того, узлы бирок удерживают информацию о местоположении и обрабатывают профиль программы с данными о характере и распорядке работы сотрудника, о его характерных рабочих функциях. Бирки могут быть запрограммированы для распознавания схем нормального использования и для подачи сигнала тревоги в случае отклонения от этих схем. Благодаря способности бирок и FPN к обработке и коммуникации, имеется доступ к функциям, которые всегда требуют использования централизованного процессора.

Данное изобретение также включает использование сетевой системы в условиях больниц, фабрик и складов, в учебных зданиях, а также при слежении за перевозимыми грузами.

ПОДРОБНОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

Система сконфигурирована таким образом, чтобы отвечать конкретным потребностям слежения или распознавания с использованием соответствующей микропрограммы для запуска второго микропроцессора (прикладного центрального процессора) и устройств ввода-вывода, связанных с микропроцессором и соответствующей конфигурацией сети для запуска третьего микропроцессора (сетевого центрального процессора).

Сообщение и взаимная связь (радио- или какая-либо другая) между несколькими FPN и/или узлом бирки образует сеть. Имеются три микропроцессора, объединенные в интегральную схему, как было описано выше, которая включает интегральную схему Neuron® 3150 производства фирм Motorola и Toshiba, которым отдается предпочтение в каждом узле бирки и FPN. В этих интегральных схемах первый микропроцессор (вышеописанный центральный процессор связи) управляет алгоритмом доступа к средствам (предсказуемый постоянный множественный доступ с контролем несущей). Второй микропроцессор управляет прикладным кодом. Последний микропроцессор управляет обработкой переменных в сети и организацией сети.

В этих оптимальных интегральных схемах с несколькими микропроцессорами каждая интегральная схема включает идентификатор (ID) на 48 бит, который хранится в постоянном запоминающем устройстве, которое обеспечивает адресацию и распознавание в сети. Согласно данному изобретению узел бирки получает сообщение от FPN или другого узла бирки, который содержит идентификационный номер узла и, таким образом, возвращает информационно направленный ответ только передающему узлу. Сообщения между разными узлами бирок и FPN могут посылаться с использованием функций подтверждения, запроса/ответа, без подтверждения и другими способами. В большинстве приложений используют функцию подтверждения, которая сообщает на посылающий узел, что его сообщение получено. Кроме того, определенные сообщения, такие как сигнал тревоги в случае вторжения или взлома, могут посылаться вне очереди, и этот приоритет, как только он становится доступным, согласно вышеописанному протоколу дает им первоочередной доступ к сети. Общий объем

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1679
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

памяти (RAM, ROM, EEPROM) в оптимальном варианте составляет как минимум 64К, что является достаточным для хранения прикладного кода и данных.

Для обеспечения дополнительного уровня безопасности некоторые сообщения могут посылаться с использованием алгоритма аутентификационного ключа. Это позволяет таким сообщениям, которые, например, пытаются изменить уровень безопасности бирки, а значит и служащего, получить подтверждение прежде, чем будут сделаны каких-либо изменения. Еще одной функцией этой системы является существование сети переменных, которая позволяет переменной из одного узла (бирки или FPN) связываться с конкретной переменной другого узла.

Кроме микропроцессоров каждый узел (тага или FPN) содержит источник питания (для узлов бирок предпочтение отдается мобильному источнику питания, например батарейке или солнечному элементу), память, приемопередатчик и определенные устройства ввода/вывода. Приемопередатчик обеспечивает коммуникационную связь между узлом и остальной сетью. Бирки сообщаются с FPN или с другими бирками с использованием радиоприемопередатчика для обеспечения бесконтактного сообщения. Это позволяет объектам и людям стать частью сети без вмешательства, а лишь находясь в пределах "зоны захвата", то есть в пределах площади, на которой действует связь. Размеры "зоны захвата" могут варьироваться в зависимости от мощности приемопередатчика и типа или размещения антенны. "Зона захвата" определяет идентичность FPN для относительного местоположения узла бирки. Подходящие радиоприемопередатчики выпускаются фирмами Motorola (R-net), Utilicom и Telxon. FPN связаны между собой при помощи монтажной схемы с двужильными шнурами, линии электроснабжения, радиосвязи, электролитов и т. п. Устройства ввода/вывода обеспечивают связь человека с биркой или FPN, такими как клавиатура и дисплей, или может обеспечивать сообщение с другими датчиками или силовыми механизмами, которые контролируются биркой или FPN.

При работе связь между отдельными узлами зависит от передачи сообщения, как показано на примере следующего чередования:

В посылающем узле прикладной центральный процессор принимает решение (на основе данных таймеров, устройств ввода/вывода и т.п.) о необходимости сообщения по сети определенной информации для других узлов в качестве "сетевой переменной", которая корректируется прикладным процессором. После обработки (которая происходит в памяти, общей для сетевых и прикладных центральных процессоров, т. е. в прикладном буфере) переменная передается сетевым центральным процессором в сетевой буфер. Затем сетевой центральный процессор модифицирует память для того, чтобы она вмещала дополнительную информацию, например адрес (входящий и исходящий), а также любую специальную информацию по сортировке, например аутентификацию. Адреса узлов системы, в которые направляются конкретные сообщения, хранятся в памяти, как во время инсталляции. Центральный процессор связи контролирует сетевые сообщения пока не очистится канал связи; в это время он передает по сети сообщение через приемопередатчик с использованием таких средств, как многожильные скрученные провода, радиочастота и т.п. Алгоритмом, используемым для определения времени передачи сообщения, является предсказуемый постоянный множественный доступ с контролем несущей.

Сообщение перемещается по сети до тех пор, пока не ослабляется до такой степени, когда его становится невозможно распознать в качестве полноценного сообщения. Только те узлы, которые находятся в пределах определенного достижимого участка сети (на основе характеристик приемопередатчика), получают правильное сообщение.

В приемном узле сообщение принимается через его приемопередатчик, если сообщение передается в центральный процессор связи. Центральный процессор связи проверяет, имеет ли полученное сообщение правильный формат. Если правильный, то оно запоминается в его сетевом буфере. Сетевой центральный процессор, зная о том, что сообщение получено, декодирует его для того, чтобы проверить, предназначено ли данное сообщение для этого узла. Если нет, то оно сбрасывается. Если да, то в случае необходимости осуществляется дополнительная проверка и обработка, то есть аутентификация и подтверждение. Новое значение сетевой переменной выделяется и проходит через прикладной буфер назад в прикладную программу прикладного центрального процессора. После этого программа использует новое значение в соответствии с параметрами конкретного приложения.

Что касается всех узлов, то существует рабочий диапазон или зона захвата, в которой бирка может сообщаться с другими узлами. Этот диапазон может быть различным в зависимости от конкретного приложения, а также типа посылаемого сообщения. Например, в приложении слежения за служащим зона захвата для FPN, контролирующего уровень безопасности служащего, ограничивается входом или пределами одной комнаты. Кроме того, если FPN следит за служащим, который хочет войти через дверь, то он посылает поисковое сообщение, которое дает доступ только к входу. Если FPN пытается определить фамилии всех служащих в комнате, посылаемое сообщение охватывает расстояние, покрывающее всю комнату. Для оптимальной работы зоны захвата различных бирок или FPN, имеющие, как правило, форму круга, могут слегка перекрываться для гарантии полного покрытия площади по крайней мере одним узлом. Прием обратного сигнала о местоположении от двух или более FPN автоматически обнаруживает бирку в перекрывающем участке между соответствующими зонами захвата.

Кроме того, в некоторых приложениях желательна связь узла интерфейса человека с сетью. В таких случаях персональный компьютер или подобное устройство может быть присоединен к сети для просмотра и изменения информации в сети, доступ к

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1680
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

которой он имеет, и может добиться сетевой связи с ней.

Если говорить точнее, в приложении слежения за служащим и контроля доступа система в оптимальном варианте выполняет следующие операции:

Пример 1 - Приложение контроля безопасности и рабочей дисциплины

Служащие носят с собой или на себе бирки, которые в памяти программы имеют информацию, которая включает опознавательные данные служащего, в частности его фамилию и идентификационный номер. Для соблюдения рабочего распорядка индивидуальные бирки обеспечивают возможность слежения за служащим на работе, сообщая о моменте его прихода, ухода и о времени, проводимом на рабочем месте, т.е. о полном рабочем времени (предположительно). Эта функция также служит для обеспечения определения местоположения конкретных служащих. Кроме того, для приложений контроля безопасности бирки содержат уровень безопасности служащего, в электронной памяти хранятся отпечаток большого пальца служащего, его личный идентификационный номер и т. д. Категория допуска в данном контексте либо конкретно уточняет, либо определяет, какие двери (а следовательно, и помещения) служащий может открыть, в какое время и в какие дни.

FPN размещаются по всему рабочему месту, предпочтительно - как минимум один на контролируемую комнату или помещение, а также вдоль коридоров, на входе и на выходе, на огороженных стоянках для автомобилей служащих. Узлы на входе и выходе постоянно посылают сообщения "поиска бирок". Бирки получают эти сообщения и срабатывают на уровень безопасности, чтобы определить, имеет ли служащий право на вход. Если такое право за ним признается, а это достигается либо соответствием уровня безопасности на тэге, либо с помощью использования личного идентификационного номера, устройство вывода FPN вызывает открывание двери. Если же одновременно нужно войти группе служащих с получением единого разрешения на открывание двери, то проверяются все бирки. Если какая-либо из бирок показывает, что служащий не имеет права на вход, то срабатывает сигнал тревоги. Реальный контроль над использованием может осуществляться служащими, которые должны гарантировать, что никто не войдет в дверь без бирки, или путем соединения FPN с устройством ввода датчика, срабатывающего на движение, который реагирует на вход без соответствующего сообщения бирки.

Когда бирка (а значит и служащий) получает разрешение на вход в здание, бирка получает и запоминает сообщения из FPN и в свою очередь запоминает время вхождения и местоположение. Когда служащий покидает помещение, FPN, расположенный над выходом, который также постоянно посылает сообщения "поиска бирок", устанавливает связь существующей бирки с существующей информацией о времени и дате. Бирка вычисляет общее время, проведенное за работой (т. е., определенное как общее время, проведенное на рабочем месте), а после этого передает вычисленное значение в FPN. Эта информация запоминается, а затем используется для платежной ведомости или с целью других оценок труда служащего.

Внутренние двери и площади помещения содержатся в безопасности по той же методике, что и внешние коридоры. Бирки могут быть запрограммированы на различные уровни безопасности на основе времени суток или характера использования. Для приложений, обеспечивающих высокий уровень безопасности, бирки имеют фотографии служащих в рамках под пленкой для визуального изучения. Кроме того, в памяти бирки хранится уникальная биометрическая информация, такая как изображение отпечатка большого пальца служащего. По запросу при входе служащий пользуется устройством для считывания отпечатка пальца для сканирования большого пальца. Изображение обрабатывается и сравнивается с изображением, хранящимся в памяти бирки. Если изображения совпадают, то дверь открывается. Если нет, то включается сигнал тревоги. Кроме того, в памяти бирки может храниться и другая биометрическая информация, например узор сетчатки и т. п. В качестве запасного варианта в бирку внесены личные данные служащего, служащему наугад задаются вопросы, касающиеся этих данных, а ответы вводятся с помощью клавиатуры. Правильные ответы открывают вход.

Для постоянного контролирования доступа в здание бирки первоначально программируются с указанием даты прекращения действия. Раз в месяц бирки сверяют с узлом проверки - узлом, который хранит в памяти текущие уровни проверки безопасности для сравнения служащих и их категорий допуска. Просроченные бирки недействительны. Субподрядчики и командированные обеспечиваются бирками соответствующей категории допуска, действительными в течение короткого срока. Если уровень безопасности бирки нужно повысить или понизить, для установления местоположения бирки по всем FPN рассылаются сообщения. Если бирки для проверки или перепроверки в пределах помещения нет, то в память каждого узла на входе на месяц или до тех пор, пока бирке не присвоят соответствующую категорию или не признают недействительной, вводят новые параметры. После этого изменения вносятся в узел проверки. По истечении месячного срока бирки автоматически становятся недействительными и могут быть возобновлены в службе безопасности с одновременным внесением всех изменений. Благодаря связи между бирками, FPN и узлом проверки изменения в бирки вносятся автоматически без необходимости сбора и возвращения бирок.

Радиоприемопередатчик не позволяет служащим снимать опознавательные значки, поэтому нет смысла брать карточки с записанными данными о времени прихода и ухода. Не нужно это и для группы служащих, имеющих доступ (т.е., если группа служащих входит в здание одновременно, то не требуется, чтобы каждый в отдельности предоставлял свой значок для активной проверки). Благодаря регистрации передвижений каждого служащего, его местонахождение известно в любое время

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1681
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

для наблюдения и передачи двустороннего сигнала вызова.

Поскольку каждая бирка закодирована уникальным распознавательным маркером, каковым является фамилия служащего или его идентификационный номер, бирка может использоваться для определения местоположения служащего или группы служащих в пределах рабочего помещения (или врача в пределах больницы и т.д.). Доступ к FPN открывается через его порт ввода/вывода с введенными опознавательными данными служащего (фамилией или идентификационным номером), и он дает сообщение о местонахождении. Это сообщение передается на FPN, который после этого делает запрос о всех бирках в зоне захвата подконтрольных участков. Бирка, местонахождение которой установлено, подтверждает прием сообщения с указанием передающей FPN. О вызове носителя бирки извещает звуковой сигнал и/или личное сообщение на жидкокристаллическом дисплее. Ближайший FPN дает новое сообщение, указывающее, что запрашиваемая бирка находится в пределах его зоны захвата, и передает его обратно исходному FPN, извещая запрашивающего о местонахождении служащего или другого персонала. Ответы подобным образом могут посылаться на основной пейджер или же любому другому уполномоченному лицу.

Узел интерфейса, приспособленного для человека (HI), способен опрашивать любой узел в сети, доступной для этого интерфейсного узла, и осуществлять выборку любой информации, хранящейся в памяти узла. Примером такой способности может служить следующий: программа, работающая в таком интерфейсном узле, позволяет менеджерам следить за местонахождением служащих. Кроме того, она позволяет менеджерам компилировать статистические данные о характере работы каждого служащего. Узел проверки, например интерфейсный узел HI, содержит все категории допуска, и менеджер или представитель службы безопасности может просматривать и вносить изменения в этот узел из такого интерфейсного узла в любое время. Таким образом, менеджер, входя в сеть, имеет список своих служащих с категориями допуска. Кроме того, бухгалтерская программа содержится в бухгалтерском интерфейсном узле, который получает информацию из узлов бирок для контроля рабочего времени (на основе времени прибытия и убытия), которая может накапливаться каждую неделю или каждый месяц. Эта информация может использоваться для составления платежной ведомости.

Далее даются другие конкретные примеры использования данного изобретения в условиях больниц, на производствах, при транспортировке грузов и в учебных заведениях:

Пример 2 Больница

Узлы бирок находятся на врачах, пациентах и других представителях персонала больницы и могут прикрепляться к основному передвижному оборудованию для выполнения различных функций, связанных с наблюдением, распознаванием и определением местоположения. Следя за местонахождением каждой из бирок, система обеспечивает функции безопасности, позволенные только уполномоченному персоналу на ограниченной площади и в ограниченное время, а также ограничивает использование и перемещение маркированного бирками оборудования.

Хотя большинство пациентов находятся в фиксированной позиции (больничная кровать и окружающая обстановка), можно наблюдать и за пациентами, которые могут передвигаться. Система последовательного наблюдения за местонахождением докторов и пациентов позволяет направлять входящие телефонные звонки на ближайший к доктору или пациенту аппарат, а значит может функционировать и как система двустороннего сигнала вызова. В одном из вариантов воплощения бирки оснащены клавишами для ввода информации, которые позволяют передавать информацию другим биркам на расстоянии, включая людей или оборудование, к которым они прикреплены, а также конкретных пациентов доктора.

В случае крайней необходимости пациенты или сестры активируют бирку, нажимая кнопку для немедленного вызова ближайшего доктора. Система может определить это путем опроса FPN, ближайших к FPN, который получает сообщение о необходимости помощи. Таким же образом персонал больницы может определить местоположение ближайшего оборудования, например аппарата для ЭКГ, набрав код такого оборудования. Экран информирует запрашивающего о ближайшем месте нахождения аппарата. История болезни пациента, которая хранится в памяти бирки, сразу же поступает в распоряжение прибывшего доктора. Информация о предписаниях врача и режиме питания также содержится в памяти для обеспечения большей точности и для извещения персонала, если пациент вовремя не получил пищу или лекарства (бирка сестры посылает подтверждающие сообщения бирке пациента о принятии извещения об отпуске лекарства или кормлении). Отсутствие подтверждающих сообщений вызывает звуковой предупреждающий сигнал бирки пациента, который извещает бирку соответствующего работника.

Пример 3 - Производство

В то время, как система может использоваться как система хронометражного учета (система рабочих листков), устройство двусторонней пейджинговой связи, средство для слежения за служащими, она также может использоваться как средство для контроля продукции и учета средств вместе с бирками служащих, которые автоматически следят за временем их прибытия и убытия и за использованием конкретной техники и выполнением определенной работы, т.е. за производительностью. Бирки на всем инвентаре, применяемом в процессе производства, позволяют следить за его использованием, информируют плановиков о его количестве и местоположении, а также наблюдать за работой на протяжении всего производственного процесса.

Бирка служащего служит для оценки степени использования работником техники для производства, а также времени оценки

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1682
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

производительности работника и стоимости рабочей силы (т. е. какова последовательность технологических операций, выполняемых каждым работником, и за какой период времени). В этом режиме бирки сообщаются с FPN. Техника, которая распознает пользующегося ею работника, автоматически приспосабливается под потребности пользователя, например для использования лицами с физическими недостатками или для конкретной последовательности технологических операций.

Бирки особых размеров со встроенной клавиатурой предусмотрены последовательностью технологических операций и перемещаются по соответствующим рабочим позициям для наблюдения за этапами процесса производства через устройства ввода/вывода, собранные данные вводятся в бирку для сравнения с формулами, которые разработаны инженерами для оптимизации внутренних и внешних свойств, хранящихся в памяти бирки. Эти данные могут использоваться для определения последовательности технологических операций. Частые отказы или значительные отклонения свидетельствуют о том, что процесс вышел из-под контроля, и наблюдающий немедленно уведомляется об этом биркой через вышеописанную связь или через непосредственный запрос бирки.

Контролирование затрат времени на различных рабочих позициях, а также запоминание информации, касающейся конкретных работников, занятых в технологическом процессе, позволяет оценить затраты и быстро и точно увязать их с конкретным технологическим процессом. Это может быть выполнено, если бирки работников будут сообщаться с бирками, связанными с технологическим процессом, и если и те, и другие будут сообщаться с FPN, связанными с техникой. Кроме того, состояние технологического процесса может оцениваться в реальном масштабе времени.

Бирка также используется при наблюдении за местоположением, количеством, возрастом и условиями окружения инвентаря. Определение местоположения инвентаря осуществляется с использованием методов, подобных описанным ранее в отношении определения местонахождения служащих. В бирки изначально загружается информация о продукте, источнике и другая идентификационная информация, а совокупность всех идентификаций бирок служит для распознавания конкретных единиц, а также обеспечивает информацию относительно количества инвентаря. В бирке изначально закодирована дата, которая позднее используется при определении возраста конкретной единицы инвентаря и таким образом обеспечивает возможность использования метода FIFO (принцип простой очереди). Соответствующие датчики, подсоединенные к устройствам ввода-вывода бирки, обеспечивают условия непосредственного окружения, такие как температура, при которой сохраняются продукты или воздействию которой они подвергаются во время хранения. При получении инвентаря данные о всех запчастях вводятся непосредственно в соответствующую бирку. Если инвентарь перестает соответствовать заранее определенным установленным параметрам, система дает сигнал на бирку агента по закупкам о необходимости восполнения запаса деталей указанного наименования.

В случае остановки производственной линии или необходимости срочных закупок двусторонняя пейджинговая связь бирок значительно повышает эффективность.

Пример 4 - Наблюдение за перевозкой грузов

При использовании на транспорте бирки прикрепляются к поездам, грузовикам или контейнерам и содержат в памяти информацию, касающуюся типа и происхождения груза, времени его доставки к месту назначения, местоположения в данный момент и т.п., таким образом создавая электронный коносамент на груз. После этого бирки сообщают о местонахождении и состоянии через установленные промежутки времени или при приближении к стационарным локационным узлам, расположенным на обочинах дороги или на грузовиках. Бирки также могут быть запрограмированы для предоставления информации о расходе топлива в реальном масштабе времени, обеспечения наблюдения за рефрижератором и т.п.

Для сообщения с датчиками массы в движении, позволяющими следить за массой груза в дороге, в бирки вносится регистрационная информация. Служащие на дорогах, мостах и у туннелей, снабженные FPN, могут считывать нужную информацию с грузовиков без необходимости их остановки. В случае необходимости входные линии бирок на грузовиках или других транспортных средствах могут быть соединены со спидометрами, автопрокладчиками, тормозами, топливомерами и т.п. для наблюдения за водителем и транспортным средством.

Пример 5 - Университетское удостоверение и пропуск

В университетских и других студенческих городках FPN размещают повсеместно для того, чтобы они могли получить сигнал опасности от человека с биркой. При нажатии кнопки на бирке FPN на территории получают сигнал опасности от бирки и триангулируют площадь для определения местоположения данной бирки. Триангуляция осуществляется FPN, который получает сигнал бедствия, связываясь с соседними узлами, чтобы определить, какие из них получили сообщения. Когда объект на территории точно указан, сигнал передается на узел приспособленного для человека интерфейса (HI) в ближайшем центре службы безопасности. Сигнал подтверждения, например гудок в бирке, подтверждает, что помощь уже в пути.

Дополнительной функцией, которой можно добиться, воспользовавшись этой же системой FPN, является функция "обхода караула", которая гарантирует прибытие охранника на установленное место в запланированное время.

Среди других примеров применения бирок - хранение в памяти идентификационных номеров студентов и служащих, а также финансовой информации для бухгалтерии.

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1683
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Эта финансовая информация может использоваться для закупок, ведения библиотечных дел и т.д. Студенты могут использовать бирку для наблюдения и контроля своих расходов и ведения бюджета. Незаконный доступ пресекается благодаря использованию аутентификационных алгоритмов.

Описанная выше функция триангуляции может быть легко использована с другими приложениями для определения местоположения конкретных предметов или людей, как этого требует локационный ввод из двух или более FPN. В этом аспекте представляется возможным обеспечить для FPN широкий диапазон связи (в зависимости от выходной мощности) для расширения радиуса действия и более эффективного использования триангуляционного определения местоположения, когда лишь один FPN пребывает в "зоне захвата".

ПОДРОБНОЕ ОПИСАНИЕ ФИГУР И ОПТИМАЛЬНОГО ВАРИАНТА ВОПЛОЩЕНИЯ ИЗОБРЕТЕНИЯ

На фигуре 1 показана блок-схема основных компонентов и деталей, связанных с биркой 1, контрольным устройством, размещенным на объекте, в соответствии с данным изобретением. Бирка 1 включает интегральную схему 2 с тремя (3) микропроцессорами 3, 4 и 5 и связанной с ними микропрограммой 6. Микропрограмма 6 включает общий протокол связи, конкретный прикладной код и конкретную конфигурацию сети для определенного приложения. Микропрограмма 6 хранится как в памяти кристалла 7, так и в навесном запоминающем устройстве 8. Интегральная схема 2 также соединяется с радиоприемопередатчиком 9. Радиоприемопередатчик принимает цифровой сигнал от микропроцессора и преобразует его в электромагнитный сигнал, который затем передается через антенну 10.

Кроме того, антенна 10 получает электромагнитные сигналы, которые передает на радиоприемопередатчик 9, который затем преобразует эти электромагнитные сигналы в цифровые сигналы, которые затем передаются на интегральную схему 2.

Каждая бирка питается от долгосрочной батарейки 12. В зависимости от конкретного применения системы интегральная схема 2 имеет различные связанные с ней устройства ввода-вывода 11. Они могут включать датчики и исполнительные механизмы, такие как клавиатура или дисплей.

На фигуре 2 показана диаграмма основных аппаратных компонентов, связанных с FPN 20. Узел 20, как определено в данном изобретении, имеет два главных компонента: узел наблюдения 22 и устройство маршрутизации 21. Источник питания 32 снабжает энергией обе части системы. Остальная часть узла наблюдения 22 идентична вышеописанному узлу бирки 2 за исключением того, что сообщения, которые осуществляются через приемопередатчик 30 с двужильным шнуром, и микропрограмма 27 изменена в соответствии с конкретным применением. Эта особая микропрограмма 27 хранится в навесном запоминающем устройстве 28 и навесном запоминающем устройстве 29. С интегральной схемой могут быть связаны определенные устройства ввода/вывода 31.

Устройство маршрутизации 21 транслирует сообщения между средствами различного типа, в данном случае - между радиоприемопередатчиком бирки и приемопередатчиком 30 с двужильной парой узла наблюдения 22. Сообщения, уходящие из узла наблюдения 22, движутся по сети 37 и принимаются приемопередатчиком 36 с двужильной парой. Этот приемопередатчик преобразует сигнал в сети 37 в цифровой сигнал, воспринимаемый маршрутизатором 35. Затем этот сигнал принимает форму, распознаваемую радиоприемопередатчиком 34, а затем распространяется как воздушные волны через антенну 33. Подобным же образом сообщения, полученные от бирки, в конечном счете поступают в сеть 37 после трансляции через устройство маршрутизации 21.

Примером применения в целях определения местоположения и обеспечения безопасности может служить изображенное на фигуре 3 устройство на входе, снабженное FPN 101, имеющим определенный радиус запроса, который может накладываться на радиус других узлов системы. Как видим, прохождение через вход служащего, имеющего на себе узел бирки 201, вызывает диалог между FPN и биркой с опросом относительно уровня допуска и удостоверения личности служащего. Если служащий имеет право на вход, замок двери 110 приводится в движение узлом 101 и открывается, чтобы впустить служащего в конкретную зону, а в бирку заносятся данные о времени и дате прибытия. По выходе из зоны узлы 101 связываются с узлом бирки 201, записывают время выхода и вычисляют общее время присутствия на рабочем месте с учетом ранее записанных данных о времени прибытия. Затем общее время передается через FPN в узел бухгалтерии для определения размера заработной платы.

Определение местоположения служащего в пределах рабочего места осуществляется сообщающимися FPN, передающими друг другу сведения о бирках, находящихся в пределах сферы их запросов, до тех пор, пока не будет установлено местоположение запрашиваемой бирки. Сведения о местоположении бирки (а также служащего) передаются запрашивающему через сеть бирок запроса.

Такой же принцип действия возможен и в отношении определения местоположения докторов, пациентов и передвижного медицинского оборудования в пределах территории больницы; а также определения местоположения инвентаря и продуктов в пределах склада или производственного помещения или для определения местоположения транспортируемых грузов, например, как было описано выше. Впрочем, понятно, что вышеупомянутые примеры использования являются лишь образцами применения данного изобретения, и поэтому допускается возможность изменений в системе, протоколах запросов и срабатывания, а также изменений в системе без отклонения от сущности данного изобретения, как определено в пунктах формулы, описанных ниже.

Формула изобретения:

1. Сетевая система для идентификации и определения местоположения, включающая

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1684
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

два или более узлов, с по меньшей мере одним программируемым, маркирующим и обрабатывающим местонахождение объекта узлом бирки и по меньшей мере одним программируемым узлом фиксированной позиции (FPN) для связи с узлом бирки для определения местонахождения, идентификации и текущего контроля за указанным узлом бирки относительно FPN, причем каждый из указанных узлов включает интегральную схему с программируемым микропроцессором, уникальный идентификационный номер, приемопередатчик для приема и отправки информации, запоминающее устройство, причем каждый узел дополнительно включает средство прямой связи между узлами и средство для самостоятельного принятия решения без участия центрального процессора, причем каждый узел дополнительно включает встроенный источник питания и средство связи с FPN или другим узлом бирки с возможностью опроса или без таковой, причем вышеуказанный FPN и узлы бирок включают средство сопряжения для установления связи с устройством ввода и вывода на бирке человека или объекта, причем вышеуказанная интегральная схема включает по меньшей мере три независимых микропроцессора с общей памятью и схемой контроля, но с раздельными наборами регистров, где первый микропроцессор включает центральный процессор связи, приспособленный для обеспечения контроля доступа к средствам и связи между узлами и имеет устройство связи с приемопередатчиком для приема и передачи информации.

2. Система по п.1, отличающаяся тем, что второй микропроцессор включает прикладной центральный процессор, способный работать с кодом, записанным по меньшей мере для одного конкретного применения по идентификации и определению местонахождения объекта, причем второй микропроцессор оснащен устройством связи со средством сопряжения для первичной обработки данных на основе окружающих условий согласно программе и для взаимодействия с человеком для ввода команды.

3. Система по п.2, отличающаяся тем, что третий микропроцессор включает сетевой центральный процессор, приспособленный для соединения прикладного центрального процессора с центральным процессором связи, причем указанный третий микропроцессор способен выполнять обработку сетевых переменных, адресацию, обработку сообщений, аутентификацию и управление сетью.

4. Система по п.3, отличающаяся тем, что сообщения между узлами осуществляются таким образом, что передающий узел знает, получено его сообщение или нет, и требуется или ожидается ответ.

5. Система по п.3, отличающаяся тем, что каждый узел содержит указанные общие запоминающие устройства, представляющие собой ЗУПВ, ПЗУ и ЭСППЗУ, причем объем памяти указанных устройств составляет по меньшей мере 64 К.

6. Система по п.1, отличающаяся тем, что в программу узлов бирок введены параметры уровня безопасности для правильного определения системой местоположения бирок и их носителей.

7. Система по п.6, отличающаяся тем, что указанные узлы бирок хранят в электронной памяти версии биометрической информации об их носителях.

8. Система по п.6, отличающаяся тем, что узлы бирок включают персональные данные об их носителях, причем указанные узлы бирок представляют случайные вопросы носителю, причем для открытия доступа на охраняемые участки, на которых узлы бирок запрограммированы соответствующими параметрами уровня безопасности, требуются правильные ответы.

9. Система по п.6, отличающаяся тем, что узлы бирок содержит средства, позволяющие осуществлять дистанционное изменение или отключение параметров уровня безопасности через указанные приемопередатчики.

10. Система по п.5, отличающаяся тем, что места с уровнями безопасности имеют детекторы движения для обнаружения входа любого лица, не имеющего узел бирки.

11. Система по п.1, отличающаяся тем, что узлы бирок приспособлены для сохранения информации о местоположении и обрабатывают профили характерных параметров труда работника по найму и времени, проведенного за работой или выполнением конкретных рабочих функций.

12. Система по п.1, отличающаяся тем, что узел бирки приспособлен для приема сообщений от другого узла, и данное сообщение содержит идентификационный номер передающего узла, причем принимающий узел возвращает информационно направленный ответ только на передающий узел.

13. Система по п.1, отличающаяся тем, что указанные узлы бирок содержат средства поискового вызова, обеспечивающие двухстороннюю дистанционную связь с их носителями.

14. Система по п.13, отличающаяся тем, что указанное средство поискового вызова включает элемент включения сигнала тревоги, который во включенном состоянии обеспечивает прием как минимум одним FPN в пределах площади сообщения сигнала тревоги узла бирки, имеющей такой элемент включения сигнала.

15. Система по п.1, отличающаяся тем, что FPN размещены по всей контролируемой площади с возможностью перекрывания зон захвата, определенных диапазоном приемопередатчиков, а также на входе и выходе, причем FPN на входе и выходе постоянно посылают сообщения "поиска бирки", а узлы бирок, которые входят в зону захвата, сообщаются с FPN и принимают и сохраняют в памяти сообщения от FPN и, в свою очередь, сохраняют время прибытия и местоположение в памяти узла бирки, причем, когда узел бирки проходит через выход, FPN постоянно посылает сообщения "поиска бирки" и, таким образом, сообщает выходящей бирке информацию о дате и времени и дате убытия, причем узел бирки вычисляет общее время работы, которое определяется по общему времени пребывания узла бирки в пределах контролируемой зоны.

16. Система по п.15, отличающаяся тем, что площадь зоны захвата может быть

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1685
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

различной в зависимости от мощности приемопередатчика, причем зона захвата определяет идентичность FPN для относительного местоположения узла бирки.

17. Система по п.1, отличающаяся тем, что узел бирки имеет специальные размеры, позволяющие использовать ее в технологическом процессе на производственном оборудовании, причем указанная бирка приспособлена для наблюдения за стадиями производственных процессов на указанном производственном оборудовании через средство сопряжения для сравнения действительных стадий производственных процессов с формулами, разработанными производственными инженерами, для оптимизации внутреннего и внешнего качества производственных процессов, которые хранятся в памяти бирки, причем отклонения фактических стадий производственных процессов от формул указывают на процесс, который вышел из-под контроля, причем указанная бирка также включает средство оповещения наблюдающего о выходе указанного процесса из-под контроля.

18. Система по п.1, отличающаяся тем, что она приспособлена для наблюдения в больницах, причем узел бирки прикреплен к конкретному пациенту, а история болезни пациента хранится в памяти бирки и доступна для врача через средство сопряжения.

19. Система по п.18, отличающаяся тем, что она включает узел бирки, прикрепленный к конкретному пациенту, причем предписания для пациента или информация о его режиме питания хранятся в памяти бирки и могут быть доступны для врача, причем указанный узел бирки содержит средство для оповещения персонала о неполучении пациентом дозы лекарства или пищи.

20. Система по п.19, отличающаяся тем, что узел бирки прикреплен к медсестре, причем указанный узел бирки медсестры оснащен устройством для передачи подтверждающих сообщений на узел бирки пациента по получении пациентом пищи или дозы лекарства, причем узел бирки пациента содержит средство звуковой сигнализации, срабатывающее в отсутствие подтверждения от узла бирки медсестры, что пища или доза лекарства приняты надлежащим образом.

21. Система по п.1, отличающаяся тем, что она приспособлена для использования в оборудовании в соответствии с требованиями заказчика, причем указанный FPN прикрепляют к указанному оборудованию, причем указанный узел бирки распознает носителя для FPN, а указанное оборудование содержит средство для приспособления его работы к требованиям указанного носителя, предварительно запрограммированное, с помощью указанной распознавательной информации от FPN.

22. Система по п.1, отличающаяся тем, что она приспособлена для учета товарно-материальных запасов, причем узел бирки предназначен для каждого объекта учета, а узлы бирок прикреплены к отдельным объектам учета, причем устройства памяти указанных узлов бирок изначально загружены распознавательной информацией, относящейся к объекту учета, к которому они прикреплены.

23. Система по п.22, отличающаяся тем, что указанная распознавательная информация включает первичную дату введения объекта в учетную ведомость для определения возраста указанного объекта учета.

24. Система по п.22, отличающаяся тем, что указанные узлы бирок содержат средство сопряжения для измерения условий окружающей среды для объекта учета.

25. Система по п.24, отличающаяся тем, что указанное средство сопряжения содержит термометр.

26. Система по п.22, отличающаяся тем, что она включает дополнительный узел, который содержит предварительно запрограммированные уровни объектов учета, причем при исчерпании запасов и удалении узлов бирок включается средство сигнализации указанного FPN, которое оповещает об уменьшении запасов.

27. Система по п.1, отличающаяся тем, что она приспособлена для наблюдения за перевозкой грузов транспортными средствами, причем ее закрепляют на указанном транспортном средстве, а в памяти указанного узла бирки хранится информация о грузе, достаточная для хранящегося в электронной памяти коносамента на груз.

28. Система по п.27, отличающаяся тем, что указанные узлы бирок запрограммированы и приспособлены для контроля за расходом топлива указанным транспортным средством в реальном масштабе времени через средства сопряжения.

29. Система по п.27, отличающаяся тем, что указанные узлы бирок запрограммированы и приспособлены для наблюдения за условиями окружающей среды для указанного груза через средства сопряжения.

30. Система по п. 27, отличающаяся тем, что указанное транспортное средство представляет собой грузовик, а указанные узлы бирок запрограммированы и приспособлены для наблюдения за работой грузовика и поведением его водителя через средство сопряжения.

31. Способ идентификации и определения местоположения объекта или человека в пределах обозначенной зоны с использованием сетевой системы по п.1, включающий а) стационарное размещение одного или более FPN в заранее определенных пунктах в пределах обозначенной зоны, причем каждый FPN имеет свой собственный уникальный идентификационный номер; б) обеспечение указанного объекта или человека одним из указанных узлов бирки, имеющим указанный уникальный идентификационный номер; в) настройку указанного FPN на передачу поисковых сообщений на указанный узел бирки с его идентификацией при помощи указанного уникального идентификационного номера, причем узел бирки имеет указанный идентификационный номер, соответствующий FPN или ближайшим к нему узлам, с получением подтверждения и идентификации FPN или узлов, получающих подтверждение, благодаря их уникальным идентификационному номеру или номерам, и определение местоположения узла бирки и объекта или человека, имеющего указанный узел бирки, относительно

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1686
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

идентифицированного FPN или узлов.

32. Способ по п.31, отличающийся тем, что человек является работником по найму, а обозначенная зона является рабочим местом работника по найму.

33. Способ по п.31, отличающийся тем, что зона является рабочим местом, а FPN размещают на выходе и входе указанного рабочего места, при этом убытие и прибытие узла бирки отмечается и хранится в указанном запоминающем устройстве указанного узла бирки с командами от связанного с ним FPN, причем указанный FPN дополнительно содержит часы/календарь для определения конкретного времени убытия и прибытия, а хранящаяся в памяти информация об указанном времени убытия и прибытия обрабатывается указанным микропроцессором для вычисления суммарного времени нахождения указанного узла бирки на рабочем месте.

34. Способ по п.33, отличающийся тем, что указанное суммарное время передается в бухгалтерию для составления платежной ведомости для работника по найму, имеющего указанный узел бирки.

35. Способ по п. 31, отличающийся тем, что человеком является врач, а указанной обозначенной зоной является больница.

36. Способ по п.31, отличающийся тем, что человеком является пациент, а указанной обозначенной зоной является больница.

37. Способ по п.31, отличающийся тем, что объектом является передвижное медицинское оборудование, а указанной обозначенной зоной является больница.

38. Способ по п.31, отличающийся тем, что объектом является объект учета, а указанной обозначенной зоной является склад, на котором хранится множество объектов учета.

39. Способ по п.31, отличающийся тем, что объектом является последовательность технологических процессов, а указанной обозначенной зоной является фабрика для производства изделий с использованием указанной последовательности технологических процессов.

40. Способ по п. 31, отличающийся тем, что объектом являются изделия, перевозимые транспортным средством, а указанной обозначенной зоной является маршрут передвижения указанного транспортного средства.

41. Способ по п.31, отличающийся тем, что указанный узел бирки сообщается с одним или несколькими FPN напрямую или с одним FPN, который, в свою очередь, сообщается с одним или несколькими FPN, причем два или несколько FPN триангулируют позицию относительно узла бирки для определения местоположения узла бирки и человека или объекта, имеющие указанный узел бирки.

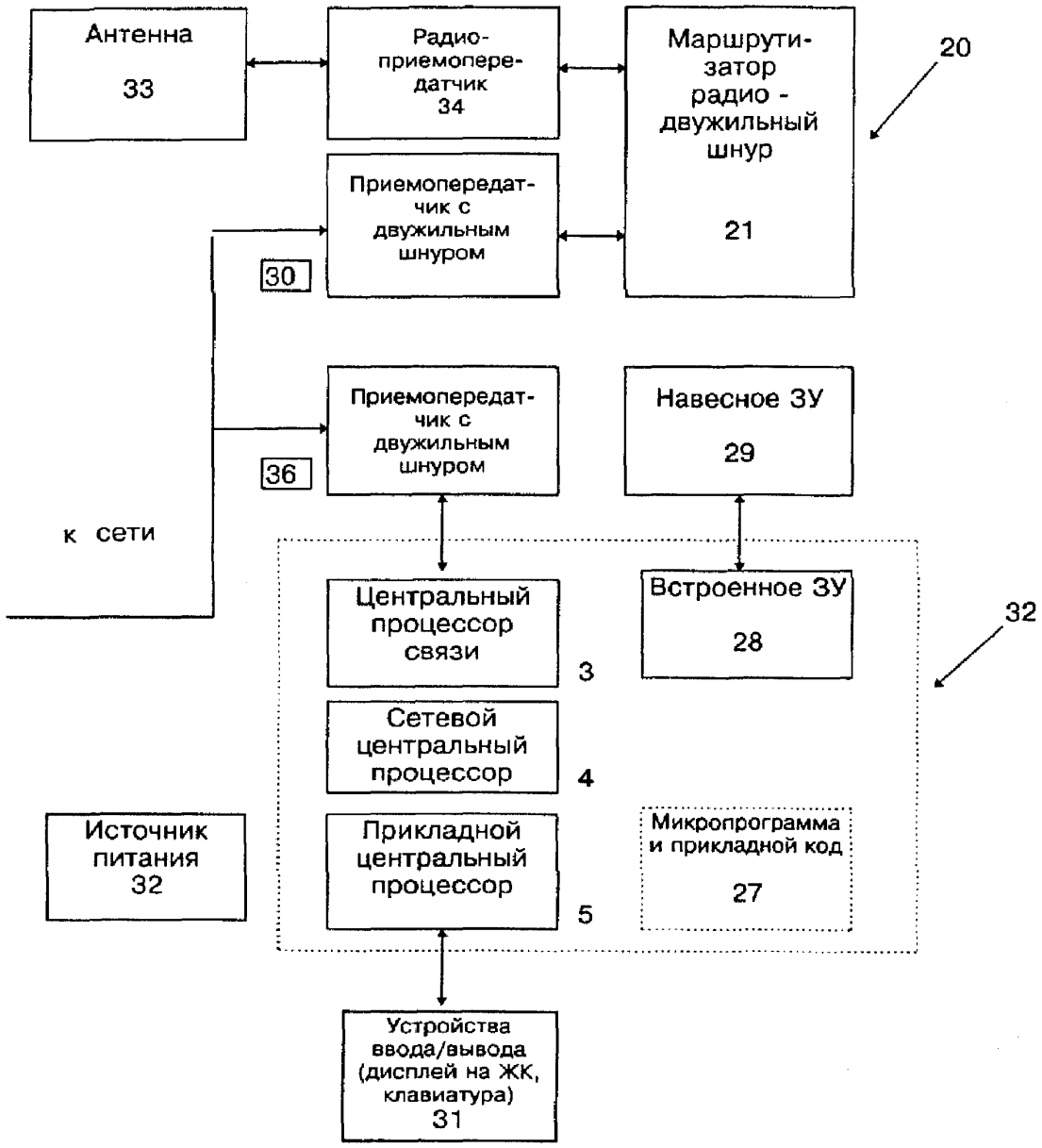
42. Способ поддержания контроля безопасности в обозначенной зоне с использованием сетевой системы по п.1, включающий а) программирование уровня безопасности на указанном узле бирки; б) программирование категории допуска уровня безопасности в FPN, находящейся в фиксированной позиции при входе в указанную зону; в) настройку указанного FPN на запрос указанного узла бирки о запрограммированном в нем уровне безопасности; г) разрешение со стороны FPN на вход в случае, если только указанный уровень безопасности соответствует категории допуска уровня безопасности или превышает ее.

43. Способ по п.41, отличающийся тем, что он приспособлен для поддержания безопасности на территории университетов и других учебных заведений, причем FPN размещают по всей территории университета для получения сигналов тревоги от лиц - носителей узлов бирок, при этом каждая бирка снабжена элементом включения сигнала тревоги, который во включенном состоянии обеспечивает прием сигнала тревоги от узла бирки хотя бы одним FPN в пределах площади сообщения, причем для определения конкретного местоположения используют триангуляции площади, при этом указанную триангуляцию осуществляют FPN, который получает сигнал тревоги, связываясь с другими соседними узлами для определения тех, которые также получили такое сообщение.

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1687
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

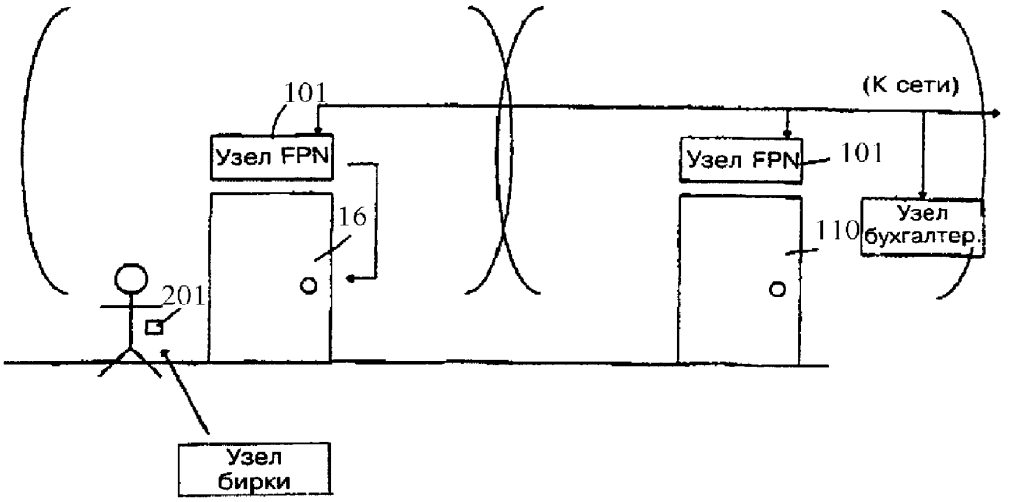


Фиг.2

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1688
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018



Фиг.3

RU 2158444 C2

RU 2158444 C2

WAVELYNX EX. 1003, Pg. 1689
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Espacenet

Bibliographic data: RU2195020 (C2) — 2002-12-20

METHOD AND DEVICE FOR USER IDENTIFICATION

Inventor(s): MINKIN V A; GREKOVICH A A; ROMANOVA L P; TATAURSHCHIKOV S S; SHTAM A I ± (MINKIN V.A, ; GREKOVICH A.A, ; ROMANOVA L.P, ; TATAURSHCHIKOV S.S, ; SHTAM A.I)

Applicant(s): MNOGOPROFIL NOE PRED OOO EHLSI ± (MNOGOPROFIL'NOE PREDPRIJATIE OOO "EHLSIS")

Classification: **- international:** ***G06F21/00; G06K19/00; G06K5/00; G06K9/00; G07F7/10;*** (IPC1-7): G06K19/00; G06K5/00; G07F7/10

- Euro: G06F21/32; G06F21/34; G06K9/00; G06K9/00A

Application number: RU20000101180 20000111

Priority number(s): RU20000101180 20000111

Also published as: EP1251448 (A1) EP1251448 (A4) EP1251448 (B1) WO0152174 (A1) WO0152174 (A8) more

Abstract of RU2195020 (C2)

FIELD: method for identifying plastic-card user. SUBSTANCE: method is implemented by device that has image reading model with light and sensor, external physical medium of fingerprint information in the form of plastic card, and data processing unit coupled with sensor in image reading module. Sensor responds to light passing both through person's finger and through plastic card, at least one of whose sides bearing visible image of at least one user's fingerprint; image reading module incorporates in addition plastic-card holder that tightly presses visible image of user's fingerprint to sensor designed for input of this fingerprint image from plastic card; light is designed to ensure uniform illumination of sensor with light passing through person's finger or plastic card. EFFECT: facilitated procedure and enhanced reliability of identifying plastic-card user. 2 cl, 4 dwg

Last updated: 24.09.2012 Worldwide Database 5.7.44.2; 92p

WAVELYNX EX. 1003, Pg. 1690
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) **RU** (11) **2 195 020** (13) **C2**

(51) МПК[7] **G 06 K 5/00, 19/00, G 07 F 7/10**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 2000101180/09, 11.01.2000

(24) Дата начала действия патента: 11.01.2000

(43) Дата публикации заявки: 27.11.2001

(46) Дата публикации: 20.12.2002

(56) Ссылки: EP 0945821 A1, 29.09.1999. RU 96124447 A1, 10.02.1999. WO 98/27509 A1, 25.06.1998. US 5987155 A, 16.11.1999. US 4582985 A, 15.04.1986. US 5473144 A, 05.12.1995. EP 0379333 A1, 25.07.1990.

(98) Адрес для переписки:
194223, Санкт-Петербург, пр. Тореза, 68, МП "Элсис", В.А.Минкину

(71) Заявитель:
Многопрофильное предприятие ООО "Элсис"

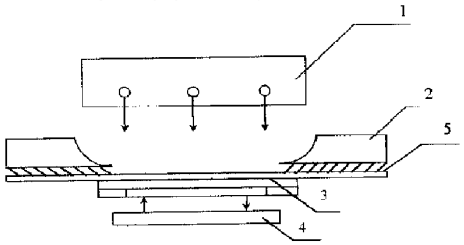
(72) Изобретатель: **Минкин В.А., Грекович А.А., Романова Л.П., Татаурщиков С.С., Штам А.И.**

(73) Патентообладатель:
Многопрофильное предприятие ООО "Элсис"

(54) СПОСОБ И УСТРОЙСТВО ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

(57)

Изобретение относится к идентификации субъекта с помощью пластиковой карты. Его использование позволяет получить технический результат в виде обеспечения простой и надежной идентификации пользователя пластиковой карты. Способ идентификации реализуется с помощью устройства, включающего в себя модуль считывания изображения с осветителем и датчиком, внешний материальный носитель дактилоскопической информации в виде пластиковой карты и блок обработки информации, связанный с датчиком в модуле считывания изображения. Технический результат достигается благодаря тому, что датчик выполнен чувствительным для света, проходящего как через живой палец, так и через пластиковую карту, по крайней мере на одной из сторон которой имеется видимое изображение хотя бы одного отпечатка пальца пользователя, а модуль считывания изображения дополнительно включает в себя держатель пластиковой карты, плотно прижимающий видимое изображение отпечатка пальца пользователя к поверхности датчика для ввода изображения этого отпечатка с пластиковой карты, причем конструкция осветителя обеспечивает равномерное освещение датчика светом, проходящим через живой палец или пластиковую карту. 2 с.п.ф-лы. 3 ил.



Фиг. 1

RU 2195020 C2

RU 2195020 C2

WAVELYNX EX. 1003, Pg. 1691
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(19) **RU** (11) **2 195 020** (13) **C2**

(51) Int. Cl.[7] **G 06 K 5/00, 19/00, G 07 F 7/10**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 2000101180/09, 11.01.2000

(24) Effective date for property rights: 11.01.2000

(43) Application published: 27.11.2001

(46) Date of publication: 20.12.2002

(98) Mail address:
194223, Sankt-Peterburg, pr. Toreza, 68, MP "Ehlsis", V.A.Minkinu

(71) Applicant:
Mnogoprofil'noe predprijatie OOO "Ehlsis"

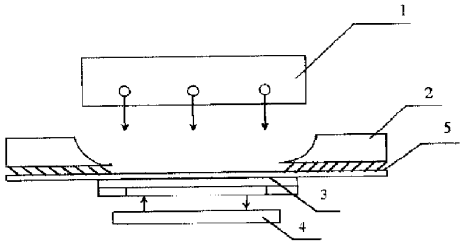
(72) Inventor: Minkin V.A., Grekovich A.A., Romanova L.P., Tataurshchikov S.S., Shtam A.I.

(73) Proprietor:
Mnogoprofil'noe predprijatie OOO "Ehlsis"

(54) METHOD AND DEVICE FOR USER IDENTIFICATION

(57) Abstract:

FIELD: method for identifying plastic-card user. SUBSTANCE: method is implemented by device that has image reading model with light and sensor, external physical medium of fingerprint information in the form of plastic card, and data processing unit coupled with sensor in image reading module. Sensor responds to light passing both through person's finger and through plastic card, at least one of whose sides bearing visible image of at least one user's fingerprint; image reading module incorporates in addition plastic-card holder that tightly presses visible image of user's fingerprint to sensor designed for input of this fingerprint image from plastic card; light is designed to ensure uniform illumination of sensor with light passing through person's finger or plastic card. EFFECT: facilitated procedure and enhanced reliability of identifying plastic-card user. 2 cl, 4 dwg



Фиг. 1

RU 2195020 C2

RU 2195020 C2

WAVELYNX EX. 1003, Pg. 1692
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Изобретение относится к электронике и может быть применено в любых областях деятельности человека, где необходимо осуществлять идентификацию пользователя. Это может быть вычислительная техника, охранные и пропускные системы, финансовая и банковская деятельность, персонализация кредитных карт, система паспортизации населения, медицина и криминалистика.

В настоящее время известен целый ряд систем идентификации пользователя, использующих для идентификации дактилоскопическую информацию с промежуточного носителя, например дактилоскопической карты. Эти системы уже около ста лет используются в криминалистике для поиска и идентификации преступников. Первоначально создается архив или база дактилоскопических карт, которая состоит из практически полного изображения отпечатка ладони и всех пальцев в отдельности, хранящегося на бумажном носителе, т.е. на обычном листе бумаги. При обнаружении следа отпечатка пальца неизвестного на месте преступления происходит съем данного следа с места преступления, его перенос на жесткий (бумажный или пленочный) носитель и дальнейший поиск данного следа по имеющейся базе дактилоскопических карт визуально или с применением мощных автоматизированных вычислительных систем [1], так называемых автоматизированных дактилоскопических систем (АДИС). Для считывания дактилоскопических карт в таких системах применяют стандартные сканеры, причем обычно электронная информация постоянно дублируется бумажными носителями.

Данные системы применяются для поиска и идентификации преступников, однако их массовое применение, например, для паспортных проектов или охранных систем затруднительно, т.к. во-первых, ввод постоянной информации связан с психологически неприятной для пользователя процедурой: нанесением слоя краски на всю ладонь, причем качество получаемых отпечатков зависит от многих факторов, и краска с ладоней снимается с трудом.

Известен способ и устройство идентификации пользователя, позволяющее осуществлять ввод изображения живого пальца без нанесения слоя краски, причем с очень высоким качеством изображения [2].

Известная система идентификации [2] включает в себя осветитель, просвечивающий палец, и сенсор с волоконно-оптической поверхностью, на которую устанавливают палец.

Свет рассеивается в пальце и проходит через кожу в местах (линиях), прижатых к оптическому волокну, с минимальными потерями, а в местах, не прижатых к оптическому волокну (ложбинах), потери света значительно больше, за счет этого и создается оптическое, а затем и электронное изображение отпечатка пальца.

Данные способ и устройство применяют для идентификации только живого пальца, т.к. описанный принцип действия применим только для рельефных объектов, причем конструкция осветителя обязана учитывать особенности рассеивания света именно в живом пальце.

Описанные особенности препятствуют разработке и созданию системы идентификации, базирующейся на едином датчике для ввода изображения как с живого пальца, так и с внешнего носителя.

Известен способ идентификации, включающий ввод постоянной информации, состоящий из следующих основных операций:

запись отпечатков пользователя в электронную базу данных, запись информации изображения в электронном виде, по крайней мере, одного отпечатка пальца пользователя на материальном внешнем носителе - чиповой пластиковой карте,

ввод оперативной информации, состоящий из следующих основных операций:

ввод изображения живого пальца в устройство сканирования, представляющее собой оптический дактилоскопический сканер с получением изображения в отраженном свете;

ввод дактилоскопической информации с чиповой пластиковой карты в устройство считывания;

сравнение постоянной и оперативной информации и вывод результатов сравнения.

Известно устройство идентификации, включающее модули считывания изображения с живого пальца и информации с внешнего носителя, выполненного в виде чиповой пластиковой карты, и блок обработки информации, причем модуль считывания изображения содержит осветитель и датчик с получением изображения в отраженном свете.

Данные способ и устройство [3] взяты нами за прототип.

Прототип позволяет осуществлять два уровня защиты объекта, используя одну дактилоскопическую информацию. Двойная защита естественно повышает уровень безопасности при допуске в систему, одновременно повышая и уровень сервиса для пользователя и уменьшая вероятность ошибок.

Данные способ и устройство сочетают все достоинства как классических систем биометрической идентификации, так и сложных пропускных систем на базе чиповых карт. Однако имеются и определенные недостатки.

Для работы устройства необходимо иметь два независимых модуля ввода информации, что несколько усложняет применение устройства. Следующим неудобством является необходимость использования относительно дорогой чиповой пластиковой карты, что особенно ощутимо при реализации массовых персонализационных проектов, таких как выдача национальных паспортов, водительских удостоверений и т.п. документов. Стоимость таких проектов будет определяться большей частью стоимостью чиповых пластиковых карт. Например, для России и 150 млн. населения выдача паспортов на базе чиповой пластиковой карты стоимостью примерно 10 USD за одну штуку составит 1,5 млрд. USD.

Использование для паспортных проектов контактных чиповых карт невозможно, т.к. несмотря на значительно меньшую стоимость (в среднем 3-5 USD за штуку) надежность работы контактных чипов недостаточна, т.к. они более легко подвержены разрушению. Известна возможность записи информации на

RU 2195020 C2

RU 2195020 C2

WAVELYNX EX. 1003, Pg. 1693
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

пластиковую карту в виде двухмерного баркода. Однако запись дактилоскопической информации или кода отпечатка содержит примерно 1 Кбайт, и двухмерный баркод такого размера по площади займет почти половину пластиковой карты. Следовательно, запись информации о двух пальцах пользователя на одну пластиковую карту практически невозможна, т.к. кроме дактилоскопической информации на ПК должно быть место и для записи демографической информации пользователя.

Другой технической проблемой является чтение двухмерных баркодов, и, следовательно, устройства чтения являются достаточно сложными и дорогими, что также препятствует использованию двухмерного баркода для записи дактилоскопической информации на ПК в массовых проектах, хотя стоимость самой ПК в этом случае и невелика ~1 USD, но стоимость оборудования для чтения двухмерного баркода в этом случае превысит стоимость изготовления ПК.

В связи с перечисленными недостатками данные устройства пока не получили массовых применений.

Предлагаемые способ и устройство позволяют просто, качественно и надежно осуществлять двухуровневую идентификацию пользователя.

Это достигается тем, что в известном способе идентификации пользователя, включающем ввод постоянной информации, содержащей запись отпечатков пальцев пользователей в постоянную базу, запись дактилоскопической информации об изображении по крайней мере одного отпечатка пальца пользователя на материальном внешнем носителе, ввод оперативной информации, содержащей ввод изображения живого пальца в устройство сканирования, ввод дактилоскопической информации с материального внешнего носителя в устройство считывания, сравнение постоянной и оперативной информации и вывод результатов сравнения, запись информации об изображении по крайней мере одного отпечатка пользователя на внешний носитель осуществляют в виде видимого изображения отпечатка пальца, а ввод изображения живого пальца и ввод информации с внешнего носителя осуществляют поочередно, устанавливая их в единое устройство считывания.

Это достигается также тем, что в известном устройстве идентификации пользователя, включающем блок считывания оперативной информации, содержащей модуль считывания изображения с живого пальца, включающий осветитель и датчик, внешний носитель дактилоскопической информации в виде пластиковой карты и блок обработки информации, датчик является сенсором, чувствительным для света, проходящего через объект, внешний носитель выполнен в виде пластиковой карты, на по крайней мере одной из сторон которой имеется видимое изображение хотя бы одного отпечатка пальца пользователя, а модуль считывания изображения с живого пальца дополнительно включает в себя держатель внешнего носителя дактилоскопической информации, плотно прижимающий видимое изображение отпечатка пальца к поверхности датчика для ввода изображения отпечатка с внешнего носителя, причем конструкция осветителя обеспечивает равномерное освещение датчика светом, проходящим через объект.

Согласно другому варианту, устройство содержит видимое изображение отпечатков пальцев пользователя, расположенные симметрично относительно центра пластиковой карты.

Еще одним отличием устройства является то, что отпечатки пальцев пользователя на пластиковой карте представляют собой бинарное черно-белое изображение.

Сущность изобретения заключается в следующем. Экспериментально установлено, что равномерное освещение пальца проходящим светом и равномерное освещение пластиковой карты также проходящим через нее светом позволяет считывать датчиком с волоконно-оптической поверхностью подобные изображения. Оказалось, что оптическая плотность стандартной пластиковой карты, изготовленной из традиционных материалов, таких как поливинилхлорид (ПВХ) или полиэстер (ПЭ) стандартной толщины 0,8 мм, примерно совпадает с оптической плотностью пальца. Для получения отчетливого изображения рисунка, нанесенного на поверхность ПК, оказалось достаточно плотно прижать рисунок, нанесенный на поверхность ПК к волоконно-оптической поверхности датчика, равномерно освещая его сверху или сбоку в проходящем через ПК светом. Относительно неожиданными в этом подходе было несколько моментов, а именно совпадение оптических плотностей живого пальца и пластиковой карты в ближнем инфракрасном свете (0,75-1,0) мкм, сходность изображений, получаемых при контакте рельефного (пальца) и плоского (ПК) объектов с волоконно-оптической поверхностью, практическое отсутствие влияния рисунков, нанесенных с лицевой стороны ПК на изображение, считываемое с обратной стороны ПК, прижатой к волоконно-оптической поверхности датчика. Положительное решение всех этих вопросов при экспериментальной проверке сделало возможным реализацию данного изобретения.

Ранее предполагалось, что для получения равномерного изображения отпечатка пальца в проходящем через палец свете палец следует освещать неравномерно, так как рассеивание света в пальце пропорционально пути прохождения света. Авторы установили, что эта зависимость существенная только для входного (в палец) диффузного света, на самом деле определяется апертурой входящего света и практически несущественна при узконаправленном световом потоке перпендикулярно плоскости датчика.

С другой стороны, наличие уже известных технических решений, способных уверенно различать изображения, получаемые с живого пальца и пластиковой карты, например, по наличию пульса [2], делает возможным широкое применение данных устройств, т.к. в противном случае вероятность подделок была бы высока. Применение одного датчика для считывания как изображения живого пальца, так и видимого изображения с карты позволяет не только упростить работу пользователя с устройством, но и

RU 2195020 C2

RU 2195020 C2

WAVELYNX EX. 1003, Pg. 1694
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

значительно повысить надежность работы системы, т. к. отпечаток, хранящийся в виде реального видимого изображения на пластиковой карте, обладает значительной помехоустойчивостью и не чувствителен к электрическим и магнитным полям в отличие от чиповой ПК. Другим преимуществом данного устройства является дополнительная возможность будущей модернизации и совместимости, заключающаяся в том, что программные алгоритмы идентификации изображения постоянно совершенствуются, причем основные изменения касаются преобразования изображения в сжатый код. В чипе может храниться только сжатый код, что не позволит или затруднит в будущем использовать новое программное обеспечение.

Хранение информации в виде реального изображения отпечатка позволит использовать все будущие улучшения программного обеспечения без минимальных затрат, причем одновременно для считывания как изображения живого пальца, так и изображения отпечатков.

Перечисленные преимущества делают возможным широкое применение предлагаемого изобретения, как для локальных систем, так и для глобальных проектов, например национальной паспортизации, авторизации доступа в Internet или дополнительной защиты кредитных карт.

Возможность расположения изображения нескольких отпечатков на одной пластиковой карте существенно повышает вероятность правильной идентификации, причем центрально-симметричное расположение отпечатков на пластиковой карте позволяет не использовать движущихся механических деталей в блоке считывания оперативной информации.

Другой возможностью повышения качества идентификации является запись и хранение на пластиковой карте не реального (полутонового), а обработанного и бинаризированного изображения, так называемого "скелета" отпечатка. Чтение "скелета" происходит с уменьшением вероятности ошибок по сравнению с чтением реального полутонового изображения.

На фиг.1 и 2 представлено предлагаемое устройство идентификации пользователя; на фиг.3 - лицевая и обратная сторона пластиковой карты.

Пример

Устройство, изображенное на фиг.1, состоит из импульсного осветителя 1, держателя пластиковой карты 2, волоконно-оптической входной поверхности датчика 3, блока обработки информации 4 и пластиковой карты 5.

В устройстве, изображенном на фиг.2, считывание изображения осуществляют тем же устройством с живого пальца пользователя 6.

В конкретном примере технической реализации импульсный осветитель, обеспечивающий равномерное освещение датчика, состоит из светодиодов марки ИРС-1-800/40, волоконно-оптической шайбы марки ИАШЮ200370002 ТУ диаметром ∅ 6 мкм одного оптического волокна, датчика типа DactoChip DC-21 и блока обработки информации в виде стандартного персонального компьютера РП-400. Связь между датчиком DC-21 и персональным компьютером осуществляется через кабель, присоединенный к параллельному порту компьютера. На компьютере установлена программа дактилоскопической идентификации DC-Enter.

Изображение лицевой и обратной сторон реально изготовленной и персонализированной пластиковой карты из поливинилхлорида со стандартными параметрами в соответствии с ISO 7810-85 и размерами в соответствии с CR80 (85 x 54 x 0,8 мм x мм x мм) приведены на фиг.3.

Аналогичная пластиковая карта, содержащая личную информацию о владельце, может являться документом, удостоверяющим личность.

Держатель пластиковой карты выполнен из металла (алюминия), на внутренней (контактирующей с пластиковой картой) стороне которого приклеен слой ворсистого материала (оптическая замша). Держатель должен плотно прижимать пластиковую карту к волоконно-оптической поверхности датчика и в то же время не допускать повреждения поверхности пластиковой карты при ее механическом перемещение между поверхностями держателя и датчика. Такая конструкция обеспечивает легкую и высокоточную установку пластиковой карты над датчиком без применения движущихся механических частей в конструкции блока считывания оперативной информации.

Устройство работает следующим образом. Первоначально была создана база, включающая информацию об отпечатках пальцев пользователей системы (работников Многопрофильного предприятия "Элсис"). Каждому пользователю была выдана пластиковая карта с его данными, образец которой приведен на фиг. 3. Два данных устройства были установлены на двери в малогабаритном герметичном корпусе, причем одно устройство контролировало вход в общее помещение, а второе - в помещение с повышенной секретностью. При входе в общее помещение пользователь устанавливает палец в датчик, прижимая его к волоконно-оптической поверхности. Датчик преобразует изображение живого пальца в электрический сигнал, который обрабатывает компьютер, проводя поиск по базе. В случае положительного результата идентификации компьютер дает команду на открывание двери. В случае отрицательного результата идентификации программа просит пользователя подтвердить свой отпечаток пластиковой картой. Пользователь устанавливает пластиковую карту в устройство считывания, датчик преобразует изображение с пластиковой карты в электрический сигнал, а компьютер проводит поиск этого отпечатка в базе и дает сигнал на открывание двери в случае подтверждения положительного результата идентификации.

Основной проблемой обычных пропускных дактилоскопических систем является высокая вероятность ошибки непропуска своего, во многом зависящая от того, что некоторые пользователи каждый раз устанавливают палец по-разному и естественно система не может их идентифицировать. Другой проблемой являются возможные повреждения или загрязнения пальцев,

RU 2195020 C2

RU 2195020 C2

WAVELYNX EX. 1003, Pg. 1695
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

которые всегда имеют место в реальной жизни. Практика показывает, что от 10 до 20% пользователей имеют сложности с дактилоскопической идентификацией, что существенно препятствует широкому распространению классических дактилоскопических систем, работающих только по живому пальцу. Использование дополнительного внешнего носителя в виде ПК с отпечатком пальца позволяет сделать вероятность идентификации близкой к 100%, а соответственно вероятность ошибки практически нулевой.

Для входа в помещение повышенной секретности пользователь вначале набирает свой персональный номер на клавиатуре, затем устанавливает палей в модуль считывания и, наконец, устанавливает ПК в тот же модуль. Дверь открывается только при совпадении всей информации, хранящейся в постоянной базе.

Возможен и другой алгоритм работы системы, когда информация об отпечатке не хранится в постоянной базе компьютера, а вводится во временную память с ПК и подтверждается живым пальцем. Это затрудняет возможность несанкционированного использования дактилоскопических данных.

Разработанные способ и устройство могут иметь самое широкое применение благодаря простоте и надежности в использовании, что было подтверждено при безотказной опытной эксплуатации данных устройств.

Список литературы

1. Рекламный проспект AFIS Sagem Morpho, Inc. www.morpho.com, 1999 год.

2. Международная заявка PCT/RU97/00105 Способ и устройство идентификации пользователя. Приоритет 19 декабря 1996 года.

3. Рекламный проспект Bio Mouse Plus, American Biometric Company, www. biomouse.com. 1999 год.

Формула изобретения:

1. Способ идентификации пользователя, включающий в себя ввод постоянной информации, заключающийся в записи отпечатков пальцев пользователей в постоянную базу и записи дактилоскопической информации об изображении по крайней мере одного отпечатка пальца пользователя на внешнем материальном носителе дактилоскопической информации, ввод оперативной информации, заключающийся во вводе изображения живого пальца в модуль считывания изображения и вводе дактилоскопической информации с внешнего материального носителя дактилоскопической информации в модуль считывания изображения, сравнение постоянной и оперативной информации и вывод результатов сравнения, отличающийся тем, что запись информации об изображении по крайней мере одного отпечатка пальца пользователя на внешний материальный носитель дактилоскопической информации осуществляют в виде видимого изображения отпечатка пальца, а ввод оперативной информации осуществляют путем поочередной установки живого пальца и внешнего материального носителя дактилоскопической информации в модуль считывания изображения для считывания одним и тем же датчиком как изображения живого пальца, так и видимого изображения отпечатка пальца с внешнего материального носителя дактилоскопической информации.

2. Устройство идентификации пользователя, включающее в себя модуль считывания изображения с осветителем и датчиком, внешний материальный носитель дактилоскопической информации в виде пластиковой карты и блок обработки информации, связанный с датчиком в модуле считывания изображения, отличающееся тем, что датчик выполнен чувствительным для света, проходящего как через живой палец, так и через пластиковую карту, по крайней мере на одной из сторон которой имеется видимое изображение хотя бы одного отпечатка пальца пользователя, а модуль считывания изображения дополнительно включает в себя держатель пластиковой карты, плотно прижимающий видимое изображение отпечатка пальца пользователя к поверхности датчика для ввода изображения этого отпечатка с пластиковой карты, причем конструкция осветителя обеспечивает равномерное освещение датчика светом, проходящим через живой палец или пластиковую карту.

RU 2195020 C2

RU 2195020 C2

WAVELYNX EX. 1003, Pg. 1696
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

RU 2195020 C2

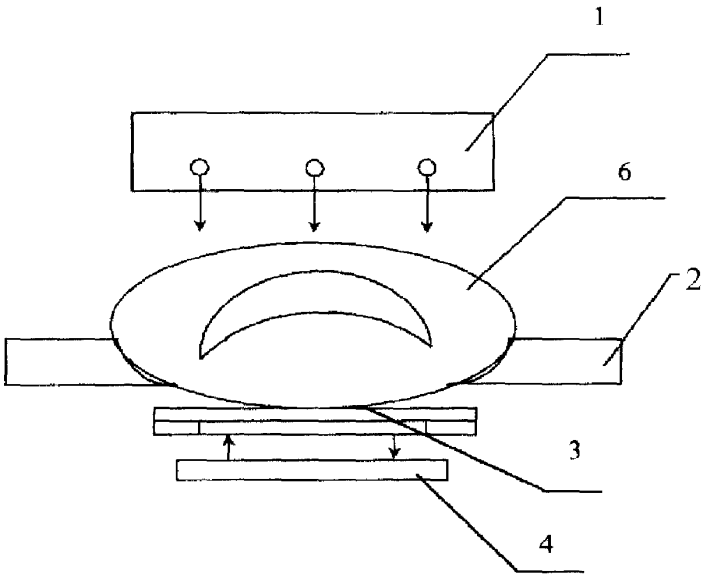
RU 2195020 C2

WAVELYNX EX. 1003, Pg. 1697
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Таблица 1

№ плавки	Содержание элементов, %																			Критерий охрупчивания K	Критерий охрупчивания Q
	C	Si	Mn	Cr	Mo	P	S	Ni	Cu	Co	V	Ti	Al	Sn	As	0	Pb	Sb	N	Fe	
1	0,05	0,14	0,28	1,4	0,35	0,006	0,006	0,06	0,01	0,01	0,008	0,025	0,05	0,001	0,003	0,0001	0,009	0,0002	0,001	остальное	21,90	0,007
2	0,07	0,15	0,30	1,5	0,40	0,001	0,001	0,01	0,01	0,005	0,05	0,01	0,005	0,0001	0,001	0,001	0,001	0,001	0,003	остальное	17,75	0,0017
3	0,10	0,28	0,80	2,0	0,80	0,003	0,004	0,15	0,02	0,015	0,30	0,08	0,01	0,0005	0,005	0,003	0,005	0,004	0,01	остальное	6,09	0,009
4	0,12	0,40	1,2	2,5	1,2	0,006	0,006	0,2	0,06	0,02	0,25	0,15	0,05	0,01	0,01	0,005	0,01	0,008	0,012	остальное	6,26	0,017
5	0,13	0,42	1,34	2,55	1,31	0,006	0,006	0,3	0,08	0,03	0,29	0,20	0,065	0,02	0,02	0,006	0,02	0,01	0,013	остальное	5,92	0,098
прототип 6	0,07	0,25	0,70	1,8	0,64	0,009	0,009	-	0,1	0,02	0,22	0,10	-	0,003	0,007	-	-	0,004	-	остальное	35,56	0,0107

WAVELYNX EX. 1003, Pg. 1698
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018



Фиг. 2



Фиг. 3

RU 2195020 C2

RU 2195020 C2

WAVELYNX EX. 1003, Pg. 1699
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G08B 13/14 — A1

(11) International Publication Number: WO 97/17683

(43) International Publication Date: 15 May 1997 (15.05.97)

(21) International Application Number: PCT/US95/14376

(22) International Filing Date: 6 November 1995 (06.11.95)

(71) Applicant: ID. SYSTEMS, INC. [US/US]; Suite 504, 325 Broadway, New York, NY 10007 (US).

(72) Inventors: LOOSMORE, N., Bert; 235 East 95th Street, New York, NY 10128 (US). EHRMAN, Kenneth; 235 East 95th Street, New York, NY 10128 (US). JAGID, Bruce; 6 Waverly Court, New York, NY 10956 (US).

(74) Agent: NISSENBAUM, Israel; Rosenman & Colin L.L.P., 575 Madison Avenue, New York, NY 10022 (US).

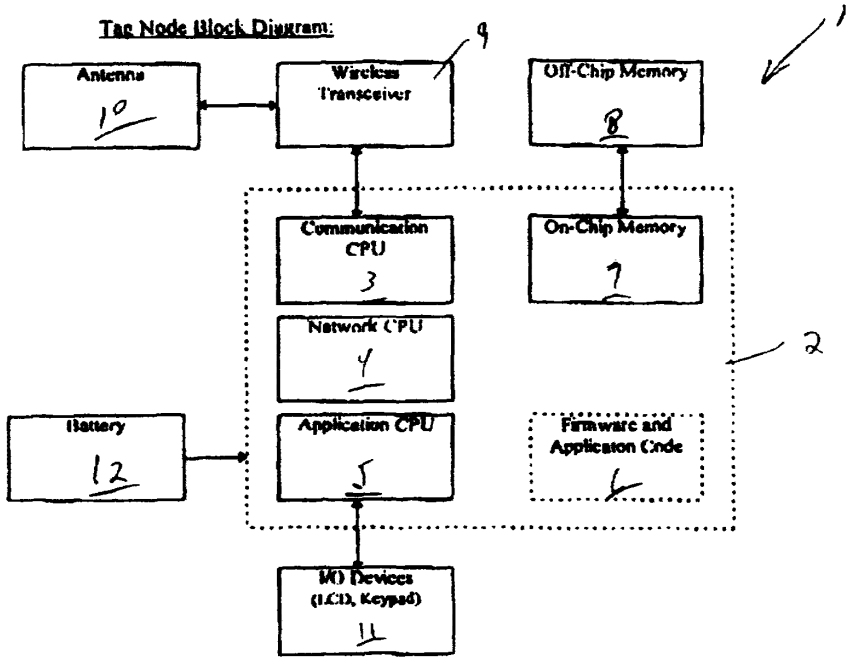
(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: ELECTRONIC CONTROL SYSTEM/NETWORK

(57) Abstract

A network system of programmable fixed position nodes (20) and movable tag nodes (1) provides direct inter-node communication capability. The individual nodes are pre-programmed to recognize external environmental conditions and to logically act on the basis of recognized condition parameters, and to communicate with other nodes. Each node comprises an IC (2) having three independent processors (3, 4, 5) which share a common memory (7, 28) and control circuitry (6, 27) but have separate sets of registers. A first processor (3) provides media access control and communication between the nodes and includes transceiver elements (9, 36) for receiving and transmitting information. A second processor (5) runs code written for the particular use, as well as the overall operating system, which is provided with direct linkage to i/o means (11, 31) for initial processing based on environmental conditions. The third processor (4) links the applications processor (5) with the communication processor (3), and handles network variable processing, addressing, etc. The nodes provide an independently operable overall network.



WAVELYNX EX. 1003, Pg. 1700
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

Electronic Control System/Network

FIELD OF THE INVENTION

This invention relates to systems for object or person identification and location, particularly systems used for employee and material tracking purposes.

BACKGROUND OF THE INVENTION

While many systems have been developed and patented for object and people identification and location, those systems have only gone so far as to allow data to be read from an encoded identification tag or for data to be programmed on the tag (read-write mode), but only in response to interrogation by a reader. Additionally, these systems have almost invariably required the use of a centralized database or centralized processor. Examples of such systems include Electronic Identification System (4,937,581 and 5,132,687) and Portable Field-programmable Detection Microchip (5,218,343). Other identification methods have been developed describing the protocol and therefore method for identifying tags, such as Electronic Identification Tag Interrogation Method (5,266,925). All of these tags have essentially been memory storage units with limited responsive capability. They have not been able to operate or react independently, based on environmental conditions, in any cognitive logical manner. Furthermore, even in network arrays there has been no interactive sharing of information between tags, or system decisional operation except through a central processing unit.

It is an object of the present invention to provide a network of programmable nodes with each having the ability to respond to specific preprogrammed external environmental conditions and to communicate with other nodes in the network by sending unrequested messages, requesting information, or alerting the system of a particular condition.

It is a further object of the present invention to provide each node in the network with a microprocessor and firmware giving the node the ability to make decisions independent of a central processing unit.

It is another object of the present invention to utilize the decision making capabilities of each node to determine the appropriate distance for each transmission in accordance with the context of the message.

It is a still further object of the present invention to utilize the network for object monitoring and location including identification in various applications.

It is yet another object of the present invention to provide a network

WAVELYNX EX. 1003, Pg. 1702
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

for monitoring various parameters including external conditions.

These and other objects, features and advantages of the present invention will become more evident from the following discussion and drawings in which:

SHORT DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating the node tag components;

Figure 2 is a block diagram illustrating the Fixed Position Node member components; and

Figure 3 is a schematic of the placement of tag and Fixed Position Node's (FPN's) for monitoring of objects or people and for identification, location, and other condition evaluation of such information.

SUMMARY OF THE INVENTION

Generally the present invention comprises a method for location and identification of objects and people, the monitoring thereof, and of system relevant parameters under situation conditions, and a method for controlling these situations. The present invention further comprises a stand-alone, parameter monitoring and evaluation system and a location and identification control system comprising two or more active operation nodes, with at least one programmable, movable identification and processing tag node or at least one programmable fixed position node (FPN). The FPN's are in known fixed positions and the tag nodes are movable, relative thereto. The relation between the fixed and movable nodes (i.e., the movable tag node relative in proximity to one or more fixed nodes) provides the location function. All nodes are initially provided with identification coding indicating where each node will be installed and who or what it is monitoring. The movable tag node is also programmed, where applicable, to monitor, store, change, and/or process environmental conditions in its varying locations.

The nodes each comprise means for direct inter-node communication and means for decision making capability, without a central processor. The tag nodes further comprise means for responsive communication to other tag nodes or an FPN via wireless communications.

The individual nodes (both movable and fixed) include an integral power source, such as a long term battery for the movable nodes and a hard wired power source for the fixed nodes. The nodes further comprise microprocessor and memory elements which are pre-programmed, where appropriate to the application, to recognize external environmental conditions and inquiries and to logically act on the basis of recognized condition parameters (received via i/o means), and means to communicate with other nodes for total or

partial network action, e.g. via transceiver means. The distance of the communication, via wireless transceiver, is determined by the microprocessor means and is related to the message being transmitted. The external environmental conditions information is attained via wireless inquiry through communication interaction from other nodes as well as from attached i/o means.

Each tag node and FPN is identified with a unique ID number by which it is uniquely addressed and identified. Each node comprises an integrated circuit, operatively controlled thereby, preferably having at least three independent microprocessors which share a common memory and control circuitry but with separate sets of registers:

In the integrated circuit, in the preferred embodiment, a first microprocessor or communication CPU provides media access control and includes linkage to transceiver means for receiving and transmitting information between the nodes (such as between the tag and an FPN, inter-tag, or FPN to FPN).

A second microprocessor is the application CPU which runs code written for the node's particular use. This second microprocessor is provided with direct linkage to i/o means for initial processing based on environmental conditions, as preprogrammed, and for human interaction for information entry and receipt. Examples of input means include keypad, condition sensors such as a temperature gauge, etc. Examples of output means include LCD display, sound alarms, and the like.

The third microprocessor, a network CPU, links the applications CPU with the communication CPU, and handles network variable processing, addressing, transaction processing, authentication, network management and the like.

The microprocessors, with additional digital circuitry and i/o and communication hardware, with particular application configuration and power source, provide components of an independently operable network in a defined area of operation capable of location identification, monitoring and logical control of preprogrammed environmental conditions and logical interaction with external inquiries for transactional operations. Specific applications include employee location within a work site. Other applications include locating doctors and equipment within a hospital, patient monitoring, product and inventory location and production monitoring within a warehouse or factory, automated time and motion studies, cargo transport monitoring and the like, and includes security applications in university settings and in

monitoring unauthorized entry in secure locations and monitoring temperature conditions of perishable inventories.

The individual nodes provide intelligent processing function. For example, in employee or personnel location applications, with security control, the tag nodes are programmed with security level parameters to enable the system to determine the proper location for the tags and the wearers thereof. Additionally, the tag nodes retain location information and process profiles of employee work habits and time spent at work or with specific work functions. The tags may be programmed to recognize normal usage patterns and to signal an alarm if such patterns are deviated from. Due to the processing and communication power of the tags and FPN's, functions which have always required the use of a centralized processor can be attained.

The present invention further comprises specific utilization of the network system for application in hospital, factory and warehouse environments, a university setting, as well as in cargo transport monitoring.

DETAILED DESCRIPTION OF THE INVENTION

The system is configured to fit the needs of a particular monitoring or identification application with the use of appropriate firmware to run on the second microprocessor (application CPU) and input/output devices attached to the microprocessor and appropriate network configuration to run on the third microprocessor (network CPU).

The communication and interconnection (wireless or otherwise) between more than one FPN and/or tag node creates a network. Three microprocessors, combined into one integrated circuit, as described above, are available and specifically include the Neuron® 3150 integrated circuit, manufactured by Motorola and Toshiba, which is preferred for use in each tag node and FPN. In these integrated circuits, the first microprocessor (communication CPU, as described above) handles the media access algorithm (predictive p-persistent CSMA). The second microprocessor handles the application code. The final microprocessor handles network variable processing and network management.

In these preferred integrated circuits, with multiple microprocessors, each integrated circuit contains a unique 48 bit ID, stored in read-only memory, which facilitates network addressing and identification. In accordance with the present invention, a tag node receives a message from an FPN or other tag node which contains the ID number of the node, and therefore returns an intelligently directed response only to the sending node. Messages between different tag nodes and FPN's may be effected by using

Acknowledged service, Request/Response, Unacknowledged, or other. Most applications use Acknowledged service which allows the sending node to know that its message was received. Additionally, certain messages, such as those alerting security of an intrusion or break-in may be given priority which, under the above protocol, grants them first access to the network as it becomes available. It is preferred that total memory (RAM, ROM, EEPROM, etc.) be at least 64K in order to allow sufficient application code and data storage.

To provide an additional level of safety, certain messages may be sent using an authentication-key algorithm. This allows those messages which, for example, try to change a tag's, and therefore employees' security level, to be confirmed before any change is made. A further function of the system is the existence of network variables, which allows variables from one node (tag or FPN) to be specifically bound to another variable of another node.

In addition to the microprocessors, each node (tag or FPN) contains a power source (for tag nodes it is preferable that the power source be mobile, such as a battery or solar cell), memory, a transceiver (transmitter-receiver) and certain input/output (I/O) devices. The transceiver provides a communications link between the node and the rest of the network. Tags communicate with FPN's or other tags by using a wireless transceiver in order to provide non-contact communications. This allows objects and people to become part of the network without intervention, by only being within a "capture zone", a range suitable for communication. The "capture zone" distance is varied based on the power output of the transceiver and antenna placement or type. The "capture zone" defines the identity of the FPN for relative location of the tag node. Suitable wireless transceivers are available from Motorola (R-net), Utilicom, and Telxon. FPN's are interconnected using a twisted pair wiring scheme, a powerline, wireless, link power solution, or the like. I/O devices provide a human interface to the tag or FPN's, such as a keypad and display, or may provide connections to other sensors and actuators the tag or FPN is adapted to monitor.

In operation, communication between separate nodes is based upon a message transfer, as exemplified by the following interchange:

In the sending node, the applications CPU decides (based on timers, i/o inputs, etc.) that it needs to send a message out over the network to communicate certain information to other nodes, as a "network variable", which the application processor updates. When updated (which occurs in the memory shared between the network and application CPU's, i.e., an application

buffer) the variable is transferred by the network CPU to a network buffer. The network CPU then modifies the memory to include other information such as address (to and from), and any special handling information such as authentication. Addresses of the nodes of the system, to which the specific messages are being sent, are stored in memory such as at installation time. The communication CPU monitors network communications until the communication channel is clear, at which time it transmits the message out over the network through the transceiver and via media such as twisted pair wires, radio frequency, etc. The algorithm used to determine when a message is being sent is predictive p-persistent CSMA.

The message travels along the network until it is attenuated by the media to the point that is unrecognizable as a valid message. Only those nodes that are within the defined reachable network area (i.e. based on the characteristics of the transceiver) will receive a valid message.

At the receiving node the message is received via its transceiver, where the message is transmitted to the communication CPU. The communication CPU makes sure that the received message contains a valid format. If so, it is stored in its network buffer. The network CPU, knowing that a message has been received, decodes the message to check whether the message was intended for that node. If not, it is discarded. If it was, additional checking or processing is performed, if necessary, e.g. authentication and acknowledgment. The new value of the network variable is extracted and passed via the application buffer back to the application program of the application CPU. The program then uses the new value in accordance with parameters of the specific application.

With respect to all of the nodes, there is a range of operation or capture zone wherein a tag in such zone can communicate with other nodes. The range varies with the particular application, as well as the type of message being sent. For example, in an employee monitoring application, a capture zone for an FPN that is monitoring employee security levels is limited to an entrance or a single room. Additionally, if the FPN is looking for employees that wish to enter the door, it sends out a seek-tag message to reach the only entranceway of the door. If the FPN is attempting to determine the names of all employees in the room, the message would be sent out a distance that covers the entire room. For optimal operation, capture zones of various tags or FPN's, of usual circular configuration, may be slightly overlapped to insure complete areal coverage by at least one node. Receipt of location feedback from two or more FPN's, automatically more

narrowly locates the tag, in the overlapping area between the respective capture zones.

In addition, in some applications, it may be desired to connect a human interface node to the network. In this case, a Personal Computer or the like may be attached to the network to view and change information on the network which it is authorized to access and with which it is capable of achieving network communications.

With more specificity, in an employee monitoring and access control application, the system operation involved is preferably as follows:

Example 1 - Security and Timecard application

Employees carry or wear tags which are programmed in memory with information which includes employee identification means, specifically the employee's name, and employee ID number. For time-keeping purposes, individual tags provide employee time tracking means by keeping track of employee's time in, time out and the amount of time at the employment site, i.e., total time worked (presumably). This function also serves to provide a means for locating specific employees. Further, for security applications, tags contain the employee's security level, an electronically stored version of the employee's thumbprint, a security PIN number, etc. Security clearance, as used in this context, either specifically details or determines which doors (and therefore areas) the employee can enter, at which times and dates.

FPN's are placed throughout the work place, with preferably at least one per room or area to be monitored, as well as along hallways, and at entry and exit locations, included gated employee parking lots. Nodes at the entry and exit locations constantly send out "seek-tag" messages. Tags receive this message and respond with their security level, in order to determine whether the employee is authorized to enter. When validated, which is achieved either by correct security levels on the tag or by the use of a PIN, the FPN output means causes the door to open for entry. However, should a group of employees enter at a single time with a single validation to open the door, all tags are still verified. A security alert is generated if any of the tags indicates that the employee is not authorized for entry. Actual monitoring of tag use can be checked by employees, where employees must ensure that no one enters a door without a tag or by coupling the FPN to a motion sensor input device to sense an entry without a corresponding tag message.

As the tag (and therefore employee) is granted access to enter the

building, the tag receives and stores messages from the FPN and in turn stores entry time and location in its memory. As the employee leaves the premises, an FPN located above the exit doorway, which also constantly sends out "seek-tag" messages, contacts the exiting tag with exiting time and date information. The tag calculates the total time worked (i.e., defined as total time within the workplace) and then passes the calculated value to the FPN. This information is stored and then used for payroll or other employee evaluation purposes.

Interior doors and areas are held secure through the same methodology as the exterior passageways. Tags can be programmed to have different security levels based on time of day or based on usage. For high security applications, the tags have employee photographs laminated to the case for visual inspection. In addition, unique biometric information, such as an image of the employee's thumbprint, is stored within the tag's memory. Upon an entry request, the employee uses a thumbprint reader to scan his or her thumb. The image is processed and compared to the stored image on the tag. A match causes the entry door to open. If not, security is alerted. In addition, other biometric information can be stored on the tag, such as retinal scan, etc. As a backup, the tag is loaded with personal data of the employee, and randomly presented questions regarding such data are put to the employee and answers are entered via a local keyboard. A correct answer permits entry.

To continually control building access, tags are initially programmed with termination dates. On a monthly basis, tags consult a validation node, a node which stores current security validation levels, to compare current employees and their clearances. Tags of terminated employees are deactivated. Subcontractors and visitors are provided with tags with short term validity of appropriate clearance. When modifications are made to a tag's security level, which can be upgraded or downgraded as appropriate, a message is sent out to all FPN's to locate the tag. Should the tag not be present in the premises for validation or different revalidation, the new parameters are stored in memory of each entry FPN for a month or until the tag is brought within appropriate range and is modified or deactivated. These changes are then updated in the validation node. If the monthly time limit expires, tags are automatically deactivated and can then be reactivated by the security office and the changes made at that time. Because of the communication link between the tags, the FPN's, and the validation node, changes to tags are made automatically without the necessity for collection

WAVELYNX EX. 1003, Pg. 1709
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

and return of tags.

The wireless transceiver allows employees not to remove ID badges from their person so that there is no need for swiping of cards with recordation of entry and exit times. Multiple swipes by groups of authorized employees are therefore also not required, (i.e., if multiple employees enter a doorway simultaneously, they are not ALL required to individually actively validate their badges). With recordation of movement of each employee, an employee's location is known at all times for monitoring and two-way paging.

Since each tag is encoded with a unique identification marker, such as employee name or employee ID number, the tag can be utilized to locate an employee or a group of employees within the work area (or a doctor within a hospital, etc.). An FPN is accessed through its i/o port with entered employee identification (name or ID number) and generates a locate message. The locate message is transmitted to all of the FPN's which then makes inquiry of all of the tags in the capture zone of the relevant areas. The located tag acknowledges receipt of the message with an indication of location to the sending FPN. An audible tone on the employee tag alerts the wearer regarding the paging and/or a message on an LCD view screen displays a personalized message. The proximate FPN creates a new message indicating that the tag in question is within its capture zone, and transmits it back to the initial FPN, advising the inquirer where the employee or other personnel are located. Responses can be similarly sent to the original pager or to any other relevant person.

A human interface(HI) node is able to poll any node on the network that is reachable from the human interface node, and retrieve any information stored in that node's memory. An example of this capability is the following: software running on such an HI node allows managers to view their employee's locations. It additionally allows a manager to compile statistics of their employees' work habits. A validation node, an example HI node, contains all security clearances and a manager or other security personnel can view and change this node at any time from such an HI node. A manager therefore, by accessing the network, has a list or his/her employees and their clearances. Additionally, accounting software is contained on an accounting HI node which receives information from the tag nodes to keep track of time worked (based on entry and exit times), which may be accumulated on a weekly/monthly basis. This information is then used for payroll purposes.

The following are further specific examples of utilization of the

present invention in the environments of a hospital, manufacturing facility, cargo transport, and a university:

Example 2 - HOSPITAL

Tag nodes are worn by doctors, patients and other hospital personnel and may also be attached to crucial movable equipment for various functions related to monitoring, identification and location. By tracking the location of each tag, the system provides security functions allowing only authorized personnel in restricted area and also limits the use and movement of tagged equipment.

Though most patients are in a fixed position (a hospital bed or surrounding environments), patients with a tendency to wander can be monitored. By consistently monitoring doctor and patient location, incoming telephone calls can be directed to the phone nearest the doctor or patient and can also thereby function as a two way paging system. In one embodiment the tags are provided with information inputting keypads to permit information to be remotely transferred to other tags, including the people or equipment to which they are attached, including a specific doctor's patient.

In an emergency situation, patients or nurses activate the tag, such as by a push-button to immediately call the nearest doctor. The system can make this determination by polling the FPN's that are closest to the FPN which receives the distress message. Similarly hospital personnel can locate the nearest equipment, such as an EKG machine by keying in a code for such equipment. A view-screen informs the requester of the nearest location of the machine. Patient history stored in the memory of a tag is immediately available to an attending doctor. Patient prescription information or feeding schedule is similarly available in memory to enhance accuracy and to alert personnel when dosages or meals are missed (a nurse's tag sends confirming messages to a patients tag as a drug or meal is dispensed). Lack of confirming messages cause the patient's tag to sound a warning and the appropriate personnel's tag is notified.

Example 3 - MANUFACTURING FACILITY

While the system can be utilized as a time card system, two-way paging device, and employee tracking means, it can also be used as a production control and cost accounting tool, with the tags worn by the employees automatically keeping track of their entry and exit times and tracking their use on specific machinery or on certain jobs, i.e. productivity. Tags on inventory and work orders throughout the production facility monitor usage,

inform planners of quantities and locations, and monitor jobs throughout the production process.

The employee tag is used for measurement of employee's use of machinery for output and time to evaluate employee performance and track labor costs (i.e. which employee worked on which workorder for what amount of time). In this mode, the tags communicate with FPN's attached to the output of the machinery. The machinery, which identifies the employee using it, is automatically customized to the user's needs, such as for accommodation of handicapped personnel, or customization for a particular work order's needs.

Tags of specialized dimensions with imbedded keypads are attached to work orders and routed to appropriate work stations to monitor stages of the production processes via i/o means, yield data is entered onto the tag, for comparison to formulas perfected by industrial engineers to optimize internal and external quality, which are stored on the tag. This data can be used to determine the routing of a work order. Failure rates or large deviations indicate a process which is out of control and a supervisor is immediately notified by the tag via the previously described communication link or by direct inquiry of the tag.

By monitoring the time spent at various workstations, as well as by storing information regarding the specific employees who worked on a work order, costs can be assessed and quickly and accurately associated with a particular work order. This is accomplished when tags associated with employees communicate with tags associated with work orders which both communicate with FPN's associated with machinery. In addition, the status of a workorder can be evaluated real-time.

The tag is also useful in monitoring inventory location, quantity, age and environmental conditions. Location of inventory is accomplished by methods similar to those previously described with respect to employee location. The tags are initially loaded with product, source, or other identification information and a summation of all the tag identifications serves to identify particular items, and also provides information regarding inventory quantity. The tags are initially encoded with a date which is later utilized in determining age of the particular item of inventory, thereby facilitating use of the FIFO method. Appropriate gauges attached to the tag i/o means provide proximate environmental conditions, such as the temperature at which the products are being stored or to which they have been subjected during storage. When inventory is issued, the data is entered directly on the appropriate tag with the parts. With pre-determined

parameters, when inventories fall below set levels, the system alerts the tag of a purchasing agent, to replenish stock of the identified item.

When a production line goes down, or when urgent issues arise, the two-way paging ability of the tag significantly increases efficiency.

Example 4 - Cargo transport monitoring

With cargo transport, tags are attached to trains, trucks or containers with stored information regarding cargo type, origin, time from destination, current location, etc., thereby creating an electronic bill of lading. The tags then communicate location and status at set intervals or with proximity location to roadside or trackside fixed location nodes. The tags can also be programmed to provide real-time fuel consumption information, refrigerator car monitoring and the like.

Registration information is stored on tags for trucks for communication with weigh-in-motion sensors to store weight, etc. Highway, bridge and tunnel authorities with FPN's can read the relevant information from the trucks without the necessity for stopping the trucks. If desired, the tags input lines on trucks or other vehicles, can be linked to speedometers, odometers, brakes, or fuel gauges, etc., to monitor driver and vehicle performance.

Example 5 - University Identification and Security Card

In a university or other campus setting, FPN's are distributed throughout the facility to receive alerts from persons wearing tags. When a button on the tag is pressed, the FPN's in the area receive the alert signal from the tag and triangulate the area to determine the specific location. The triangulation is accomplished by the FPN which receives the distress signal communicating with those around it to determine which ones have received the message. When the area is pinpointed, the signal is transmitted to a HI node at the closest security center. A return confirmation signal, such as an audible tone on the tag confirms that help is on the way. An additional function that is attained by using the same FPN grid is a "guard-tour" function to ensure that guards reach their sentry points at the scheduled times.

Other uses for the tag include storage of student or employee ID number and university account information. This account information can be used for on-campus purchases, and library transactions, etc. Students can use the tag to monitor and track their spending habits and keep a budget. Unauthorized access will be eliminated by using the authentication algorithms.

The triangulation function, described above can be readily utilized

with other applications to specifically locate items or people as required by location input from two or more FPN's. In this aspect it is possible to provide the FPN's with variable communication ranges (based on power output) to permit extension of range to more effectively use the triangulation location, where only one FPN is within the "capture zone".

DETAILED DESCRIPTION OF THE DRAWINGS AND THE PREFERRED EMBODIMENT

Referring first to FIG. 1 there is shown a block diagram of the basic hardware components associated with the tag 1, the control device located on an object, in accordance with the present invention. The tag 1 includes an integrated circuit 2 with its three (3) microprocessors 3, 4, and 5, and their associated firmware 6. Included in the firmware 6 is the general communications protocol and the specific application code and specific network configuration for the particular application. The firmware 6 is stored in both on-chip memory 7 and off-chip memory 8. The integrated circuit 2 is also coupled to the wireless transceiver 9. The wireless transceiver takes a digital signal from the microprocessor and converts it into an electromagnetic signal which is then transmitted via the antenna 10.

Additionally, the antenna 10 receives electromagnetic signals which it passes to the wireless transceiver 9, which then converts these electromagnetic signals to digital signals which are then passed to the integrated circuit 2.

Each tag 1 is powered by a long life battery 12. Depending on the particular application of the system, the integrated circuit 2 will have various input/output (I/O) devices 11 associated with it. These may include sensors and actuators, such as a keypad or display.

FIG. 2 depicts a block diagram of the basic hardware components associated with the FPN 20. The node 20, as defined in the present invention, has two main components: the monitor node 22 and the router hardware 21. The power supply 32 means provides power to both parts of the system. The remainder of the monitor node 22 is identical to the tag node 2 above except that communications occur through a twisted pair transceiver 30 and the firmware 27 is changed to be specific to the particular application. Its specific firmware 27 is stored in on-chip memory 28 and off-chip memory 29. Associated with the integrated circuit may be certain I/O devices 31.

The router hardware 21 translates messages between different media types, in this case between the wireless transceiver of the tag and the twisted pair transceiver 30 of the monitor node 22. Messages leaving the

monitor node 22 travel along the network 37 and are received by the twisted pair transceiver 36. This transceiver converts the signal on the network 37 to a digital signal understandable by the router hardware 35. This signal is then modified into a form recognizable by the wireless transceiver 34 and is then propagated to the airwaves via the antenna 33. Similarly, messages received from the tag are eventually placed upon the network 37 after being translated through the router 21.

As an example of a location and security application, in Figure 3, an entranceway is fitted with FPN's 101 having a specified range of inquiry, which may overlap with the range of other nodes in the system. As shown, an employee passing through the entranceway, and wearing tag node 201 causes an interrogation conversation between the FPN and the tag regarding security level clearance and employee identity. If authorized, a lock for door 110 is actuated by the node 101 and opens to admit the employee to the specific area and a record is entered on the tag of the time and date of entry. Upon exit from the area, nodes 101 converse with the tag node 201, note the time of exit, and calculate the total time of presence at the work site from entrance data previously written on the tag. The total time is then transmitted, via the FPN, to an accounting node for determination of pay.

Location of an employee within the work site is accomplished by linked FPN's conversing regarding the tags within their ambit of inquiry until the tag in question is located. The location of the tag (and the employee) is transmitted via the network of inquiry tags to the requester.

Similar types of operation are possible with respect to location of doctors, patients and movable medical equipment within a hospital setting; and location of inventory and products within a warehouse or factory setting; and for location of cargo transport of goods, etc. as described above. It is understood however that the above examples of utilization are exemplary of the utilization of the present invention and that changes in the system, inquiry and response protocols, and components of the system are possible without departing from the scope of the present invention as defined in the following claims.

WAVELYNX EX. 1003, Pg. 1715
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

What is claimed is:

1. An identification and location network system comprising two or more nodes, with at least one programmable, location marking and processing, movable tag node, and at least one programmable FPN for communication with the tag node, for the location, identification and monitoring of said tag node relative to the FPN; said nodes each comprising an integrated circuit with programmable microprocessor means, a unique identification number, transceiver means for receiving and sending information, memory storage means, and wherein each node comprises means for direct inter-node communication and means for decision making capability, without a central processor, with the tag node further comprising an integral power source and means for communication with an FPN or other tag node with or without interrogation; and said FPN's or tag nodes comprising interface means for interfacing with human or object input and output.

2. The identification, location and monitoring system of claim 1, wherein said integrated circuit comprises at least three independent microprocessors which share a common memory and control circuitry but with separate sets of registers, wherein a first microprocessor comprises a communication CPU adapted to provide media access control and communication between the nodes and includes linkage to the transceiver means for receiving and transmitting information.

3. The identification and location system of claim 2, wherein a second microprocessor comprises an application CPU, adapted to run code written for the particular use, as well as the overall operating system, wherein the second microprocessor is provided with direct linkage to i/o means for initial processing based on environmental conditions, as preprogrammed, and for human interaction for instruction entry.

4. The identification and location system of claim 3, wherein a third microprocessor, comprises a network CPU, adapted to link the applications CPU with the communication CPU, and wherein said third microprocessor is adapted to handle network variable processing, addressing, transaction processing, authentication, and network management.

5. The identification and location system of claim 1, wherein the tag nodes are programmed with security level parameters to enable the system to determine proper location for the tags and wearers thereof.

6. The identification and location system of claim 5, wherein said tag nodes electronically store versions of the biometric information of the wearers thereof.

7. The identification and location system of claim 5, wherein tag nodes contain personal data of the wearers thereof and said tag nodes present random questions to the wearer, with correct response being required for entry to security protected sites to which the tag nodes are programmed with appropriate security level parameters.

8. The identification and location system of claim 5, wherein the tag nodes comprise means for permitting remote changing of the security level parameters or deactivation thereof, via said transceiver means.

9. The identification and location system of claim 5, wherein locations with security levels have motion detectors to detect entry of anyone not wearing a tag node.

10. The identification and location system of claim 1, wherein the tag nodes are adapted to retain location information and process profiles of employee work habits and time spent at work or with specific work functions.

11. The identification and location system of claim 1, wherein a tag node is adapted to receive a message from another node, which message contains the ID number of the sending node, whereby the receiving node returns an intelligently directed response only to the sending node.

12. The identification and location system of claim 1, wherein said tag nodes further comprise paging means for permitting remote bi-directional paging of the wearer thereof.

13. The identification and location system of claim 12, wherein said paging means comprises an alarm actuating member, which, when activated, causes at least one FPN, in a communication area range, to receive an alarm signal from a tag having such alarm actuating member thereon.

14. The identification and location system of claim 4, wherein messages between nodes are effected by using Acknowledged service, Request/Response, Unacknowledged, or other, to allow the sending node to know its message was received.

15. The identification and location system of claim 4, wherein each node comprises memory means comprised of RAM, ROM, and EEPROM, and wherein the memory of said memory means is at least 64K.

16. The identification and location system of claim 1, wherein the FPN's are placed throughout an area to be monitored, with potentially overlapping inquiry capture zones, determined by the range of the transceivers, and at entry and exit locations, wherein FPN's at the entry and exit locations constantly send out "seek-tag" messages, whereby, when tags nodes which enter the capture zone communicate with the FPN and receive and

store messages from the FPN and in turn store entry time and location in the tag node memory, whereby, as the tag leaves through an exit, an exit FPN, is constantly sending out "seek-tag" messages, and thereby contacts the exiting tag with exiting time and date information, and wherein the tag node calculates the total time worked, defined as the total time the tag node was present within the monitored area.

17. The identification and location system of claim 1, wherein the capture zone distance is varied based on the power output of the transceiver, whereby the capture zone defines the identity of the FPN for relative location of the tag node.

18. A monitoring system comprising at least one tag node of claim 1, wherein said tag is of specialized dimensions suitable for attachment to a work order in a manufacturing facility, and wherein said tag is adapted to monitor stages of production processes in said manufacturing facility via i/o means, for comparison to formulas perfected by industrial engineers to optimize internal and external quality, which are stored on the tag, whereby failure rates or large deviations indicate a process which is out of control, and whereby said tag further comprises means to notify a supervisor of said out of control process.

19. A monitoring system for use in a hospital comprising at least one tag node of claim 1, wherein said tag node is affixed to a specific patient and wherein the health history of the patient is stored in the memory of a tag for availability to an attending doctor via the i/o means thereof.

20. A monitoring system for use in a hospital comprising at least one tag node of claim 1, wherein said tag node is affixed to a specific patient and wherein patient prescription or diet information is stored in memory of said tag node for availability to an attending physician and wherein said tag node comprises means to alert personnel when dosages or meals are missed.

21. The monitoring system of claim 20, wherein a tag node is affixed to an attending nurse and wherein said nurse's tag node is provided with means to send confirming messages to a patient's tag node as a drug or meal is being administered to said patient and wherein said patient's tag node, with lack of confirming messages, comprises means to thereupon sound a warning.

22. A monitoring system for use in customizing operation of machinery, comprising at least one tag node of claim 1, and an FPN, wherein said FPN is attached to said machinery, and wherein said tag node identifies the wearer thereof to the FPN and wherein said machinery comprises means to adapt its operation to requirements of said wearer, preprogrammed therein, with said

identification information from the FPN.

23. A monitoring system for use in inventory control, comprising at least one tag node of claim 1 for each item of inventory, and at least one additional node, wherein the tag nodes are attached to individual items of inventory and wherein the memories of said tag nodes are initially loaded with item identification information relating to the item of inventory to which it is attached.

24. The monitoring system of claim 23 wherein said identification information includes the initial date of introduction of the item to inventory to permit age determination of said item.

25. The monitoring system of claim 23, wherein said tag nodes comprise i/o means for measuring environmental conditions for the item of inventory.

26. The monitoring system of claim 25, wherein said i/o means comprises a temperature gauge.

27. The monitoring system of claim 23, wherein said other node comprises preprogrammed inventory level parameters, wherein with depletion of inventory and removal of tag nodes, inventory depletion warning means of said FPN are activated.

28. A monitoring system for use in monitoring transport of cargo via transport means, comprising at least one tag node of claim 1 attached to said transport means, and at least one other node, with the memory of said tag node containing stored information regarding the cargo, sufficient to provide an electronically stored bill of lading.

29. The monitoring system of claim 28, wherein said tag nodes are programmed and adapted to monitor real-time fuel consumption of said transport means via its i/o means.

30. The monitoring system of claim 28, wherein said tag nodes are programmed and adapted to monitor environmental condition for said cargo via its i/o means.

31. The monitoring system of claim 28, wherein said transport means comprises a truck and wherein said tag nodes are programmed and adapted to monitor performance of the truck and a driver thereof via its i/o means.

32. A method for the identification and location of an object or person within a designated area, utilizing the network system of claim 1, comprising the steps of:

a. fixedly deploying one or more FPN's at predetermined location points within said designated area, with each FPN having its own unique identification number,

WAVELYNX EX. 1003, Pg. 1719
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

b. providing said object or person with one of said tag nodes having a unique identification number,

c. causing said FPN's to send seek messages to said tag node with identification thereof, by said unique identification number, with the tag node having said unique identification number responding to the FPN or nodes closest thereto with an acknowledgment response, and

d. identifying the FPN or nodes receiving the acknowledgment response by means of the unique identification number or numbers thereof; thereby locating the tag node and object or person having said tag node relative to the known node.

33. The method of claim 32, wherein the person is an employee and the designated area is a workplace for the employee.

34. The method of claim 32, wherein the FPN's are located at an exit and an entrance of said workplace whereby exit and entry of the tag is noted and stored in said memory storage means of said tag with instructions from an FPN in communication therewith, said FPN further comprising clock/calendar means to relate said exit and entry to a specific time, and wherein the stored information of said exit and entry times is processed by said microprocessor means to calculate the cumulated time of said tag being present in the workplace.

35. The method of claim 34, wherein said cumulated time is transmitted to accounting means for payroll determination for the employee having said tag node.

36. The method of claim 32, wherein the person is a doctor and the designated area is a hospital.

37. The method of claim 32, wherein the person is a patient and the designated area is a hospital.

38. The method of claim 32, wherein the object is a movable medical device and the designated area is a hospital.

39. The method of claim 32, wherein the object is an item of inventory and the designated area is a warehouse containing a plurality of items of inventory.

40. The method of claim 32, wherein the object is a work order and the designated area is a factory used for production of items with direction from said work order.

41. The method of claim 32, wherein the object comprises items being transported by transport means and said designated area is the route for said transport means.

WAVELYNX EX. 1003, Pg. 1720
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

42. A method for maintaining security control of a designated area utilizing the network system of claim 1, comprising the steps of:

a. programming a security level on said tag node,

b. programming a security access level on an FPN in fixed position adjacent an entrance of said designated area,

c. causing said FPN to inquire of said tag node regarding the security level programmed thereon, and

d. said FPN permitting access to said entrance only if said security level matches or exceeds the security access level.

43. A method for maintaining security in a university or other campus setting, utilizing the network system of claim 1, wherein FPN's are distributed throughout the university to receive alerts from persons wearing tags, and wherein each tag is provided with an alarm actuating member, which, when activated causes at least one FPN, in a communication area range, to receive an alarm signal from the tag, whereby triangulation of the area may be effected to determine the specific location, said triangulation being accomplished by the FPN which receives the distress signal communicating with those around it to determine which ones have also received the message.

44. A method for locating a person or object having a tag node thereon, utilizing the network system of claim 1, comprising the steps of the tag node communicating with two or more FPN's directly or between a tag node and one FPN which in turn communicates with one or more other FPN's, and wherein the two or more FPN's triangulate a location position, relative to the tag node, for location of the tag node and the person or object having the tag node thereon.

WAVELYNX EX. 1003, Pg. 1721
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Figure 1 - Tag Node Block Diagram

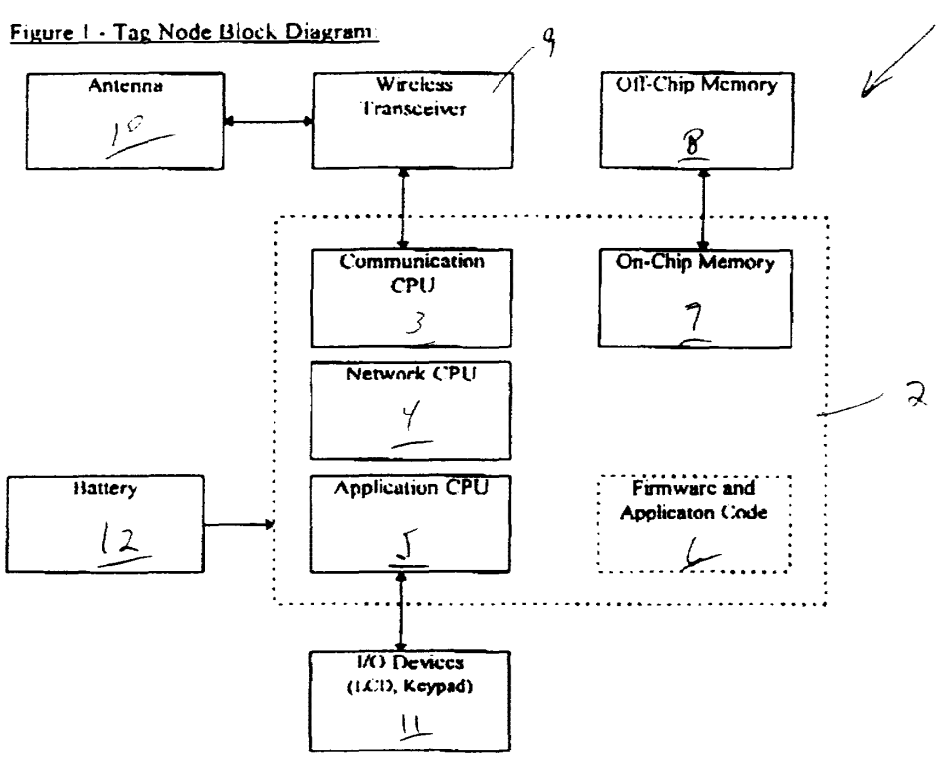
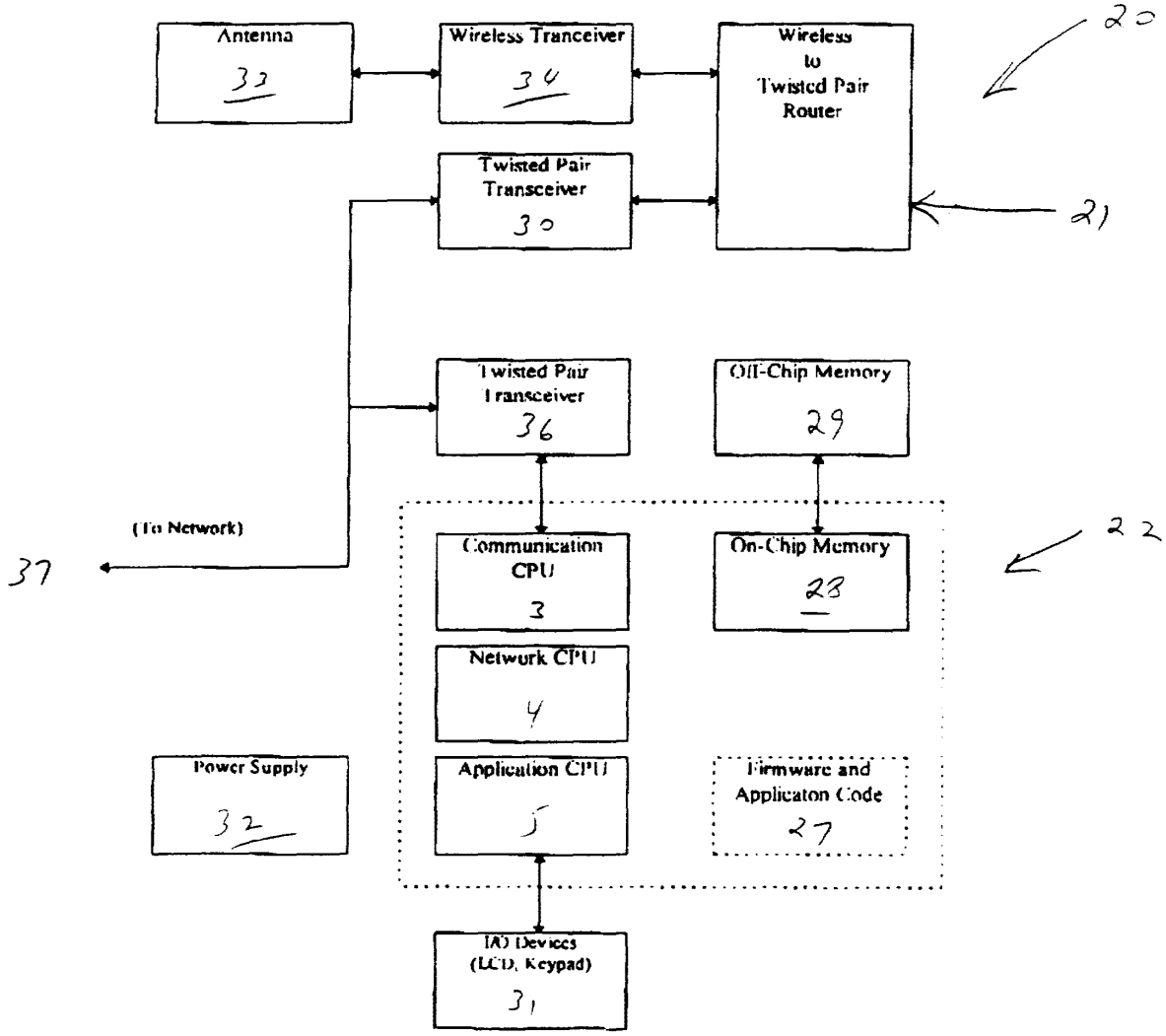
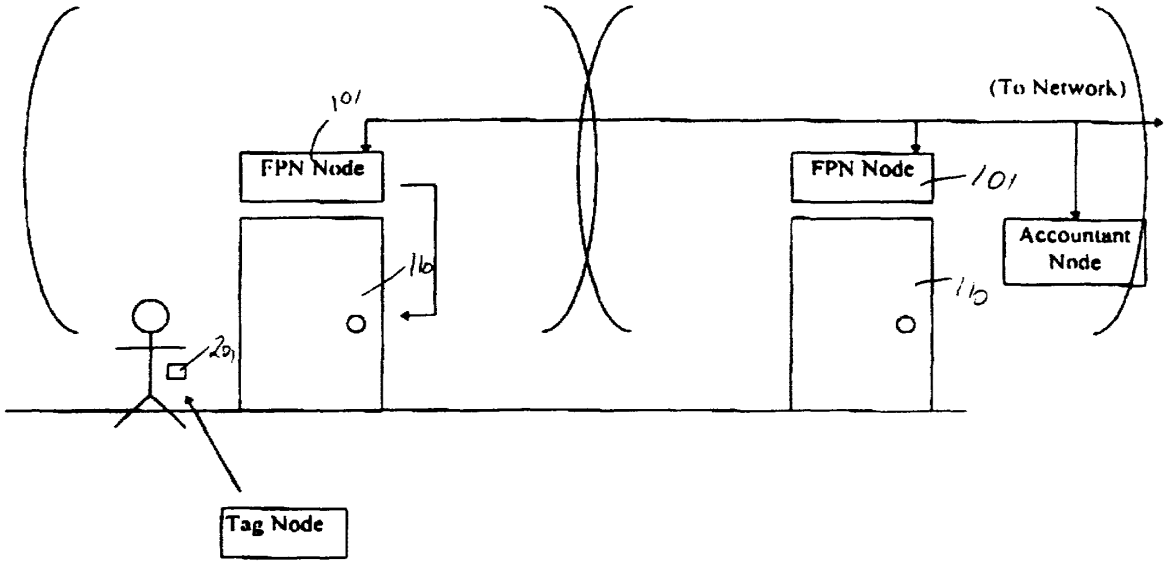


Figure 2 - Fixed Position Node Block Diagram:



Note: Twisted pair connection is optional and Communication CPU may be directly linked to Wireless Transceiver which then connects to "Network" via the antenna to create a wireless network.

Figure 3 - Capture Zone Schematic:



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/14376

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G08B 13/14
US CL :340/572, 825.49; 342/44
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 340/572-574,539,584,825.44,825.49,825.31-825.34; 342/450,44; 364/403; 235/382,385; 382/124; 379/37-38; 455/88,49.1

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US, A, 4,656,463 (ANDERS ET AL.) 07 April 1987. See cols. 4-5, 7-12, 22-24, 26, 29, 32, 37 and 43, and Figs. 5, 7, 10 and 26.	1, 11, 23-32, 39, 41, 43-44 ---------- 5-10, 12-13, 16-22, 33-38, 40, 42
Y	US, A, 5,426,425 (CONRAD ET AL.) 20 June 1995. See col. 4, lines 51-53 and col. 6, lines 20-31.	5-9, 18, 40, 42
Y	US, A, 5,151,684 (JOHNSEN) 29 September 1992. See Fig. 5 and col. 7, lines 58-65.	6
Y	US, A, 4,549,264 (CARROLL ET AL.) 22 October 1985. See col. 6, lines 39-57.	10, 16-17, 33-35

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
23 FEBRUARY 1996	14 MAR 1996
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer THOMAS J. MULLEN, JR. Telephone No. (703) 305-4382

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/14376

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,218,344 (RICKETTS) 08 June 1993. See col. 6, line 55.	12-13
Y	US, A, 4,688,026 (SCRIBNER ET AL.) 18 August 1987. See Fig. 1 and col. 8, lines 27-60.	19-21, 36-38
Y	US, A, 5,396,215 (HINKLE) 07 March 1995. See the Abstract and Fig. 3.	22

Form PCT/ISA/210 (continuation of second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/14376

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

APS (microprocessor, transceiver, programmable, computer, microprocessor, integrated circuit, IC, CPU, triangulation, cargo, shipping, freight, billing, lading, accounting, tag, transponder)

WAVELYNX EX. 1003, Pg. 1727
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 9/00, H04Q 1/00

A1

(11) International Publication Number: **WO 99/56429**

(43) International Publication Date: 4 November 1999 (04.11.99)

(21) International Application Number: PCT/US99/08990

(22) International Filing Date: 26 April 1999 (26.04.99)

(30) Priority Data:

09/066,643	24 April 1998 (24.04.98)	US
09/298,326	23 April 1999 (23.04.99)	US

(71) Applicant: IDENTIX INCORPORATED [US/US]; 510 North Pastoria Avenue, Sunnyvale, CA 94086 (US).

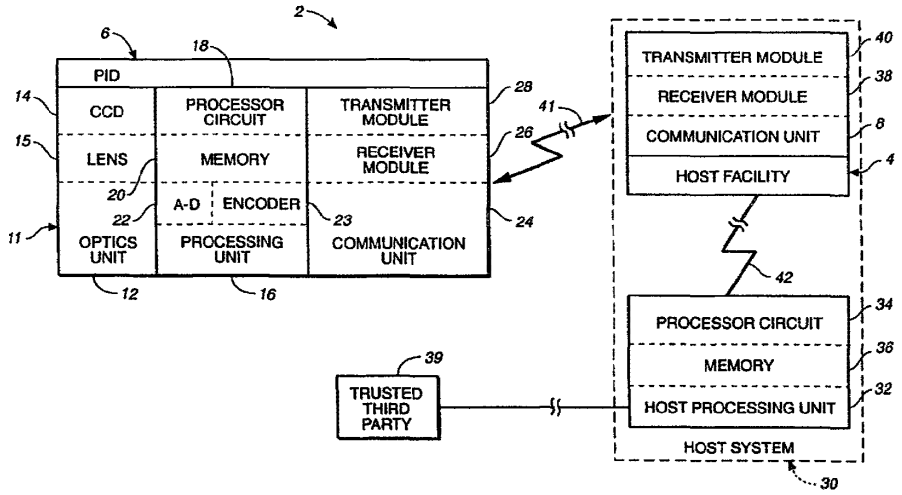
(72) Inventors: SCOTT, John, D.; 9 Pine Valley Road, Galson, NSW 2159 (AU). CURTIS, Terence, P.; 10 Selina Avenue, Kariong, NSW 2250 (AU).

(74) Agent: GARCIA, Edouard, A.; Fish & Richardson P.C., Suite 100, 2200 Sand Hill Road, Menlo Park, CA 94025 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: PERSONAL IDENTIFICATION SYSTEM AND METHOD



(57) Abstract

A portable, hand–held personal identification device (6) and method for providing secure access to a host facility (4) includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative of the sensed biometric trait. A processing unit responsive to the biometric signal is adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is unique to the enrolled person, and to provide a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person. The verification signal (41) includes information indicative of the enrolled person or the device. A communication unit, including a transmitting circuit (28), is adapted to transmit the verification signal to a host system (30).

WAVELYNX EX. 1003, Pg. 1728
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

PERSONAL IDENTIFICATION SYSTEM AND METHOD

Background of the Invention

The invention relates to a personal identification system and method for allowing access to secure facilities.

Some security systems, such as home security systems and door locks, require a user to enter a fixed code into a device at a host facility before allowing a person access to the facility. Other systems, such as automated teller machines (ATM), require a person to submit an authorized card and also to enter a fixed code that is associated with the person's bank accounts. Automobile alarms, locks, and disabling devices, and garage door openers can be operated by pressing a button on a small remote device to transmit a coded signal to a receiving unit on the automobile or garage.

Each of these security systems can be operated by any person who is in possession of the fixed code, the card or the transmitting device, as the case may be. Therefore, each of these systems is inherently insecure. Where absolute security is essential, some host facilities employ a biometric sensor to measure a biometric trait of a person requesting access to the host facility. The biometric trait is a unique identifier of a person, and can be, for example, a person's fingerprint, voice pattern, iris pattern, or the like. The requesting person also enters other identifying information about himself. The measured biometric trait is compared with stored biometric data associated with the identified person and, if there is a match, the requesting person is allowed entry or access to the host facility.

In presently available biometric systems, each authorized person registers with the host facility by providing a sample of their biometric trait, for example, by having his fingerprint optically scanned into a host system data base. Each host facility must have a biometric sensor, access to the database of registered persons' biometric trait registration data, and a processing system capable of quickly searching the database and conducting the comparison to verify a person's identity. However, if the set of authorized persons is large, such a system would require a huge database to store the fingerprint images of all the authorized persons, and the

identification process would become slower as the set of authorized persons increases.

Summary of the Invention

According to one aspect of the invention, a portable personal identification device for providing secure access to a host facility includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative thereof. A processing circuit responsive to the biometric signal is adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person. The processor provides a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person. The verification signal is indicative of the enrolled person or the device. A communication unit, including a transmitter circuit, is adapted to transmit the verification signal to a remote host system.

In another aspect, the invention features a personal identification system, comprising: a biometric sensor configured to extract a representation of a biometric trait of a user; a processor configured to verify the user's identity based upon a comparison of a representation of a biometric trait extracted from a user with a stored representation of the biometric trait; and a transmitter configured to transmit a verification signal indicative of a successful verification of the user's identity.

Embodiments may include one or more of the following features. The processor may be configured to process signals received from a global positioning system (GPS) receiver. The processor may be configured to derive trip information (e.g., the location of the GPS receiver) from the signals received from the GPS receiver. The processor may be programmable to prompt the user for additional verification information when the GPS receiver is positioned at a particular location.

The system may include a user input configured to enable a user to enter trip information, and wherein the processor is configured to process information

received from the user. The transmitter may be further configured to transmit signals representative of stored trip information.

The biometric sensor, the processor, and the transmitter may be housed within a portable, hand-held housing. The system may include an input device mounted inside a vehicle and coupled to the vehicle's power system, and wherein the input device is adapted to receive the verification signal from the transmitter and to enable the user to turn on the vehicle only upon receipt of the verification signal. The housing may have the form of a pocket-sized security badge. The housing may be configured to receive a graphical representation of the user.

The system may include an automatic door locking device coupled to a vehicle door (or trunk) and adapted to unlock the door (or trunk) upon receipt of the verification signal. The system also may include a receiver. The processor may be operable to switch the system from a low power operation to a normal power operation when the receiver receives a power-up signal from a host system. The system also may include a memory configured to store the representation of the biometric trait. The memory may be housed within a portable housing separable from the biometric sensor, processor and transmitter.

The communication unit preferably is adapted for remote communication with the host system via a wireless communication medium. The device can further include a display and a keypad.

The biometric sensor system can include a fingerprint sensor, a voice sensor, or any other type of biometric sensor. The fingerprint sensor can include a platen adapted for placing a finger thereon. The fingerprint sensor can further include an optical image sensor, which may include a complementary metal oxide semiconductor (CMOS) optical sensor, a charge coupled device (CCD) optical sensor, or any other optical sensor having sufficient resolution to provide a signal indicative of a fingerprint image. In the embodiments with an optical sensor, the platen would include an optical platen, and the biometric sensor may also include a lens focusing light from the platen onto the optical sensor. The fingerprint sensor can alternatively include a direct contact sensor device, such as a capacitive sensor chip or thermal sensor chip. In these embodiments, the platen would be the surface of the sensor chip.

The processing unit can include a processor circuit, a memory and an encoder, wherein the memory stores the biometric data, and wherein the verification signal includes an encrypted signal encrypted by the encoder. In one embodiment, the encoder includes an encoding circuit, and the verification signal further includes an ID code indicative of the enrolled person or the device.

In another embodiment, the encoder comprises an encryption algorithm programmed into the processor. The encryption algorithm employs a private key indicative of the enrolled person or the device. In this embodiment, the communication unit can further include a receiver circuit. The memory can further store an ID code indicative of the enrolled person or the device. The processor unit can be further adapted to first cause the transmitter circuit to transmit an ID code signal indicative of the ID code to the host system. The receiver circuit can be adapted to receive a host response signal transmitted by the host system in response to the ID code signal. The processor unit employs the encryption algorithm and the private key to encrypt the host response signal to create the verification signal, and causes the transmitter circuit to transmit the verification signal to the host system only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person.

In either of these embodiments, the memory can be located in a removable plug-in module, and the personal identification device further includes a socket adapted to receive the module.

According to another aspect of the invention, a portable, hand-held personal identification device for providing secure access to a host facility includes a housing. A fingerprint sensor system in the housing is capable of sensing a fingerprint of a user and providing a fingerprint signal indicative thereof. The fingerprint sensor system includes a platen on a surface of the housing adapted to receive a finger. A communication unit in the housing is adapted for wireless communication with a separate host system. The communication unit includes a transmitting circuit and a receiving circuit. A slot in the housing receives a removable smart card that includes a memory. The device can be combined with the smart card. The memory in the smart card stores a fingerprint template representative of the fingerprint of an enrolled person, and an ID code and a

personal encryption key being associated with the device. A processing circuit in the device is adapted to cause the ID code signal from memory to be transmitted by the transmitting circuit. The processing circuit is further adapted to cause a host response signal received by the receiving circuit signal from the host system in response to the ID code signal to be encrypted according an encryption algorithm employing the personal encryption key and to cause the encrypted host response signal to be transmitted by the transmitting circuit only if the fingerprint signal corresponds sufficiently to the fingerprint template to verify that the user is the registered person.

According to yet another aspect of the invention, a method of providing secure access to a host facility includes the step of registering one or more persons with the host facility, including storing a unique ID code and a public encryption key for each registered person. The method also includes receiving a first transmission comprising a first user signal at the host facility, generating and then transmitting a random number signal from the host facility only if the first user signal represents one of the stored ID codes, receiving a second transmission comprising a second user signal at the host facility, decrypting the second user signal with the public encryption key associated with the registered person who is also associated with the stored ID code represented by the first user signal, and providing access to the host facility only if the decrypted second user signal represents the random number.

According to still another aspect of the invention, a method of providing access to a secure host facility only to registered persons includes registering one or more registered persons with the host system. Registering each registered person includes storing an ID code associated only with a portable hand-held device under the control of that registered person. The method also includes transmitting an ID code signal from a portable hand-held device to a host facility of the host system. The ID code signal represents an ID code associated with the transmitting device. Other steps include generating, at the host facility, a random number signal representing a random number in response to the ID code signal only if the ID code signal is representative of the ID code of the device controlled by one of the registered persons, and retrieving, with the host system, a public key associated

with the one of the registered persons only if the ID code signal is representative of the ID code of the one the devices controlled by the one of the registered persons. Retrieving the public key can include retrieving the public key from a trusted third party. Further steps include transmitting the random number signal from the host facility to the transmitting device, and receiving the random number signal with the transmitting device. The method also includes generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of the transmitting device, and comparing, with the transmitting device, the user fingerprint signal to a fingerprint template stored in the transmitting device, wherein the fingerprint template represents a fingerprint image of a person who is enrolled with the transmitting device. Other steps include encrypting the random number signal with the transmitting device, the random number signal being encrypted according to an encryption algorithm employing a private key associated only with the transmitting device, transmitting the encrypted random number signal from the transmitting device to the host facility only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person, decrypting the encrypted random number signal with the host system, including employing the retrieved public key, and providing the user access to the host facility only if the decrypted encrypted random number signal represents the random number.

Transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each can include transmitting via a wireless transmission. Transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each can further include transmitting via at least one of a modem, a cable access TV line, and a computer communication medium.

In yet another aspect of the invention, a method of providing a secure function at a host facility only to a registered person includes registering a person with the host facility by storing an ID code associated only with a portable registered device controlled by the registered person, learning a synchronization counter of the registered device, storing an encryption key associated with the

registered device and associating the encryption key of the registered device with the stored ID code. The method also includes generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of a portable user device, comparing, with the user device, the user fingerprint signal to a fingerprint template stored in the user device, the fingerprint template representing a fingerprint image of an enrolled person who is enrolled with the user device, and generating an access signal with the user device only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person, the access signal including an ID code associated only with the user device, button press information representing a requested function, and encrypted data encrypted with an encryption key associated with the user device, the encrypted data including a synchronization counter associated with the user device. The method then includes transmitting the access signal from the user device to the host facility, determining, with the host facility, if the ID code in the access signal matches the stored ID code, retrieving the encryption key of the registered device if the match is successful, employing the encryption key of the registered device to decrypt the encrypted data and determine the synchronization counter of the user device, comparing the synchronization counter of the user device with the synchronization counter of the registered device, and providing the requested function represented by the button press data only if the synchronization counter of the user device matches the synchronization counter of the registered device.

In another aspect, the invention provides a method of accessing a secure host facility, including sensing a biometric trait of a user that is unique to a user with a biometric sensor system of a portable device, and providing a biometric signal indicative of the biometric trait; comparing, with the portable device, the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person; providing a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person; and transmitting the verification signal and an ID code signal to a remote host system, wherein the

ID code signal is indicative of an ID code associated only with the portable device, and wherein the host system provides access to the secure facility in response to the verification signal only if host facility determines that personal device associated with the ID code belongs to a registered person.

The system can be employed to provide secure access to a variety of different types of host facilities. The system can be used to replace security systems employing key card entry, fixed code entry, or a combination of key card and fixed code entry, which are currently employed, for example, with ATM's, gate and garage door openers, burglar alarm systems, point of sale (POS) devices, hotel room locks, and the like. The system can also be configured for use with automotive remote key entry (RKE) systems, automotive alarm systems, and automotive immobilizers.

The personal identification device and system of the invention has several advantages. The system is very private. Persons' biometric data, such as a fingerprint, are not stored in a central database, as with prior art systems using fingerprint identification for security. An electronic template of a user's fingerprint is stored only with their own personal identification device, and is used only for verifying the user's fingerprint. In the embodiment with two-way communication, the host facilities store only an ID code and a public key for each registered person. The ID code may be the serial number of the device, and the public key can be retained by a trusted third party. The private key used by the device is never disclosed.

The personal identification device is compact, being about the same size as an electronic pager. With advances in technology, it could be made even smaller. The personal identification device can be configured such that all the information that is associated with the user, i.e., the ID code, the personal encryption key, and the fingerprint template, is stored in a smart card, which can be transferred between identical devices having the image capture electronics, processing circuit, communication module and power supply. This enables the user to switch devices when one is worn out or broken without having to re-register.

The host system can be installed at host facilities with a minimal expenditure compared with current systems employing fingerprint identification for

security. The biometric sensor is installed in each personal identification device, rather than with the host facility. This configuration also makes retrofitting existing security systems for use with the personal identification device a relatively simple procedure. The point of contact is with the personal identification device, which makes the present system more feasible for use at exposed, public locations, such as with automated teller machines, parked automobiles, and gate entries, where the weather and vandalism can be problems. This also makes the system of the invention more sanitary than other systems that require a person to operate a public terminal, keypad, or fingerprint scanner.

Because each user carries his own fingerprint template in the personal identification device, users can "roam" to many different applications and host facilities without the need to enroll the template at each site. They only need to register prior to use. This can be done over the phone or over computer communication lines, such as the Internet, if only medium level security is required.

The user has total control over the procedure for accessing a host facility. The ID cannot be read unless the user presses the fingerprint reader. The random number transmission and the encrypted random number transmission cannot be "scanned" as the random numbers are different each time access to a host facility is requested. The personal identification device can be used in conjunction with conventional telephone lines or computer network communication lines without any risk of theft.

Personal identification devices could be sold via any retail outlet, for example, as a shrink wrap product. As the units are manufactured with unique ID codes and private keys there is no need to control the sale in any way.

Unlike prior art biometric identification systems, the user is already enrolled by the first use of the personal identification device. This completely eliminates the delays and problems associated with enrolling large numbers of users and storing each user's biometric data.

Other features and advantages will become apparent from the following description, including the drawings and the claims.

Brief Description of the Drawings

FIG. 1 is a block diagram of a security system according to the invention.

FIG. 2 is a block diagram of another embodiment of a security system according to the invention.

FIG. 3. is a perspective view of a personal identification device according to another feature of the invention.

FIGS. 4A, 4B, 4C, and 4D are respective front, side, top and bottom views of an embodiment of a personal identification device.

FIGS. 5A and 5B are respective front and side views of another embodiment of a personal identification device.

FIG. 6 is a front view of a third embodiment of a personal identification device.

FIG. 7 is a flow diagram illustrating an embodiment of a method of accessing a host facility with a personal identification device.

FIG. 8 is a flow diagram illustrating another embodiment of a method of accessing a host facility with a personal identification device.

FIG. 9 is a schematic diagram of an embodiment of the processor unit.

FIGS. 10A and 10B are a perspective and block diagrams, respectively, of a personal identification system.

FIG. 11 is a perspective view of a personal identification system clipped to a user's pocket.

Detailed Description

Referring to FIG. 1, a security system 2 provides access to one or more secure host facilities 4 only to registered persons. A host facility 4 may be a bank, a store, a military base, a computer system, an automobile, a home security system, a gate, or any other facility where it is desired to restrict access to selected individuals. Each registered person uses a battery powered, portable personal identification device (PID) 6, which communicates with a communication unit 8 located at each host facility 4. PID 6 is small enough to carry on ones person, being similar in size to a hand-held pager. An example of a PID 6 is shown being held in the palm of a man's hand 10 in FIG. 3.

PID 6 includes a biometric sensor. In the described embodiment, a biometric sensor 11 includes an optics unit 12 having a CMOS optical sensor imaging device 14, and an exposed optical platen 15. Imaging device 14 can also be a CCD imaging device. A lens (not shown) may also be used to focus an image from a surface of platen 15 onto imaging device 14. PID also includes a processing unit 16. Processing unit 16 includes a processor circuit 18, an external memory 20 and may include an analog-to-digital converter circuit (A/D) 22. Some CMOS optical sensors provide a digital output signal, which eliminated the need for A/D 22. PID 6 further includes a communication unit 24, which has a transmitter module 26 and a receiver module 28.

Memory 20 stores information that is specific to processing unit 16. Memory 20 stores an ID code that is set in PID 6 by the manufacturer. The ID code of a device, which may be the device serial number, is unique to each device. Memory 20 also stores a fingerprint template that is generated by processing unit 16 from a fingerprint image signal provided by optics 12 unit when an individual first enrolls into PID 6, as will be described in detail below. That fingerprint image signal is representative of an image of a fingerprint of the enrolled individual. The fingerprint template is a data set that is representative of features of the enrolled individual's fingerprint. The fingerprint template is normally not changed once it is established in memory 20. In some embodiments, PID 6 may include a serial port (not shown), which can be used to plug into a computer to update or change the fingerprint template. For security purposes, PID 6 would be used to perform an identification verification before allowing such a change.

Processing unit 16 also includes an encryption algorithm incorporated into an encoder 23. In the embodiment illustrated in FIG. 1, the encryption algorithm is programmed into processor circuit 18. A private key that is stored in memory 20 is used with the encryption algorithm for encryption. The private key can be set into memory by the manufacturer, and is specific to each PID 6. Different PIDs 6, which have different processing units 16, will typically have different private keys. The encryption algorithm, on the other hand, can be the same for all PID's 6.

Host facility 4 is part of a host system 30. Host system 30 will typically be bank ATM systems, point of sale systems, and the like. Host system 30 also

includes a host processing unit 32, which has a processor circuit 34 and memory 36. Communication unit 8 in host facility 4 includes a receiver module 38 and a transmitter module 40. Host processing unit 32 may be located with host facility 4, or may be located at a remote location, where it may also serve other host facilities 4 in a distributed network 42.

Memory 36 stores ID codes of enrolled individuals who have registered with host system 30. Memory 36 also stores public keys associated with respective ones of the stored ID codes. By employing the correct public key associated with a specific ID code, host processor circuit 34 can decrypt a signal that has been encrypted according to the encryption algorithm and personal key associated with the specific ID code, in a manner known in the encryption arts. The public key can also be stored with a trusted third party 39, which provides this service for several host systems in a known manner.

Signals 41 may be transmitted between PID 6 and host facility via any wireless transmission method. Transmission can be via RF, infrared, induction, sound, or the like. In this embodiment, PID communication unit 24 and host communication unit 8 will normally have a short transmission range of approximately a meter or less, however, longer ranges can be used as well. Hard-wire transmission methods can also be employed, either alone or in combination with a wireless transmission method. For example, transmission can employ dial tone modulation frequency (DTMF)(tone transmission) via a conventional phone system, employ a cable TV line in conjunction with the cable remote control system, or employ a computer communication medium, such as the Internet or a private network. PID 6 can employ more than one transmission/reception mode, such as, for example, an RF and a DTMF unit.

In another embodiment of a security system 2A, shown in FIG. 2, a PID 6A includes most of the features of PID 6 described above with reference to FIG. 1, with some significant differences. Note that features that system 2 has in common with system 2A are labeled with the same reference numerals in FIGS. 1 and 2, which convention is continued in the remainder of the FIGS. and in the following description. One difference is that communication module 24A lacks receiver module 26. Also, encoder 23A includes an encoder chip, for example, the HSC200

or HSC300 KEELOQ® Code Hopping Encoder, available from Microchip Technology, Inc. of Chandler, Arizona, that contains the encryption algorithm. Security system 2A includes a host facility 4A in which host processing unit 32A is located at the same site as host facility 4A. Host system communication unit 8A includes a receiver module 38, but does not include a transmitter module.

The embodiment illustrated in FIG. 2 will typically be employed with systems such as garage door openers, automobile security systems, door locks, and the like. As such, PID communication module 24A will have a longer transmission range than communication module 24 in the embodiment illustrated in FIG. 1.

Encoder 23A includes an ID code, which may be a serial number of encoder 23 or PID 6A. Encoder 23A also includes a synchronization counter, an encryption key and an encryption algorithm that employs the encryption key. Host system 4A must "learn" the ID code and the synchronization counter for each PID 6A which is used to access a function of host system 4A. Host system 4A must also know the encryption key.

Referring now to FIGS. 4A-4D, one embodiment of a PID 6B, which includes all the features also shown in FIG. 1, includes a housing 44 similar in size to a personal pager or a small cellular telephone. A front side 46 includes a keypad 48 for entering data and commands, and a liquid crystal display 50 for displaying data being entered with keypad 48 and for displaying status signals to the user. Keypad 48 can be eliminated in some models where programmability is not required. Platen 15 is located at the top of PID 6B, and is contoured for a finger. Platen 15 is also slightly recessed in housing 42 to provide some protection from scratching. A back side 56 of PID 6B includes a battery cover (not shown) and apertures for a DTMP speaker (not shown). A serial port can be included under the battery cover.

Housing 42 includes a slot 52 for receiving a smart card 54, which is shown in shadow being fully inserted into slot 52 in FIG. 4A. Smart card 54 includes external memory 20, and can be removed from one housing 42 and used in a new housing 42. Because memory 20 contains all the personal information, i.e., the private key, the ID code, and the fingerprint template, the smart card can be used with a different PID housing 42 without having to re-enroll the user or re-register

any user information with host systems. Some models in which memory 20 is hard-wired inside housing 42 would not include smart card slot 52.

FIGS. 5A and 5B illustrate an embodiment of a PID 6C in which keypad 48 and smart card slot 52 are not included. PID 6C does, however, include platen 15, display 50, and a belt clip 58, which could be included in any model.

FIG. 6 illustrates an embodiment of a PID 6D which is structured similar to the embodiment illustrated in FIG. 2, for uses such as a garage door opener or automobile security system. PID 6D includes platen 15 at the top of housing 42, and three function buttons. For an automobile security system the function buttons can be a driver door button 60, a trunk button 62 and an alarm button 64. Buttons 60, 62, and 64 can be adapted for use with other host systems having different functions.

Optics unit 12 can be an image sensor module available from Fingerscan PTY Ltd (an Identix company), of Sydney, Australia, as part of their F3 OEM Kit. The entire F3 OEM Kit manual, published in 1998, is incorporated herein by reference. Platen 15 and imaging device 14 have a usable area of about 16 mm X 18 mm. Imaging device 14 in the F# OEM kit is a CMOS device that provides a video output comprising an analog fingerprint image signal representing an image of a finger placed on platen 15. The fingerprint image signal is communicated to processing unit 16 via a six-wire connector 68, which is shown in a circuit diagram illustrated in FIG. 9.

Most of processing unit 16 is also included in the F3 OEM Kit. Referring again to FIG. 9, processor circuit 18 includes an SH7034 32-bit RISC microprocessor 70, made by Hitachi of Japan. Microprocessor 70 communicates over an 8-bit data bus 72 with external memory 20 and A/D 22, and over control lines 74, 76 with optics unit 12. The SH7034 microprocessor 70 has a 64 Kb internal programmable read only memory (PROM) engine and an internal 4 Kb static random access memory (SRAM).

In the PROM resides a Fingerscan Biometrics Engine (FBE), which includes algorithms for capturing and processing fingerprint image signals. These algorithms allow a finger image of approximately 140 Kbytes to be converted into a finger model, or template, of approximately 120 bytes. This size saves memory

and improves the speed of processing by decreasing the time it takes to transfer finger models to and from the internal memory. The FBE includes special instruction sequences to optimize the following operations: image capture and background rejection; video signal filtering and digitizing; template matching; finger presence detection; false finger detection; and power on self test.

A/D 22 converts the analog video signal from optics unit 12 into digital data that is stored in memory for subsequent use by processor circuit 18. Memory 20 also stores the finger template of the user who is enrolled in PID 6, and also stores custom written code. Microprocessor 70 controls and has access to 1 Mbyte in DRAM 78 -70) and 512 Kbytes of external flash memory in PROM 80. DRAM 78 includes two NEC 424400 chips, and PROM 80 is an AMD 29F040 chip.

In one embodiment of communication unit 24, transmitter module includes an induction loop data link, which is configured as a short-range (< 0.5 m) wireless modem, operating at 1200 Baud, at 70 KHz carrier frequency, using amplitude shift keying modulation. The protocol is half duplex, carrier detect multiple access (modified aloha) and the software includes a CRC 16 packet error correction method. A processor included in transmitter module is based on a PIC16C72 device. The transmit current is typically 1 mA.

In the embodiment illustrated in FIG. 9, encoder 23 resides in code programmed into processing circuit 18. However, as discussed above, other embodiments may base encoder 23 on a dedicated encoder chip, such as the HSC200 or HSC300 KEELOQ® Code Hopping Encoder. A PID may include encryption code residing in processor circuit 18 and also include an encoder chip so that PID can combine the functions of the embodiments illustrated in FIGS. 1 and 2 in a single unit. These encoder chips combine a 32-bit hopping code generated by a non-linear encryption algorithm, with a 28-bit serial number and 6 information bit to create a 66-bit transmission stream. The length of the transmission eliminates the threat of code scanning, and the code hopping mechanism makes the transmission unique, thus rendering code capture and resend schemes useless.

An owner of PID 6 must first "enroll" into the unit. Enrollment is the process of scanning a finger to create an image which is stored as a fingerprint template in memory 20. The user enrolls on the unit by removing the "packing"

cover and placing a thumb or finger on platen 15. PID can be configured to automatically start the enrollment routine with this action. Enrollment takes approximately 7 seconds. The resultant template is stored in memory 20. Ideally, PID 6 is configured to enable a user to enroll one finger on each hand so that, if the user injures the finger they usually use for verification, an alternate image is available.

Enrollment preferably permits the user several attempts to check and test the operation on the verify. Instructions and queries would be indicated, for example, by display 50 in this mode (see FIG. 4A). Until the user accepts the enrollment the unit will not transmit signals in any way but will allow any number of attempts to re-enroll and verify (test) the operation. Once committed there is no going back or editing.

If the enrollment is be stored on a removable smart card 54 (see FIG. 4A) along with the ID code and private encryption key files, these would not be accessible to other devices. It allows users to swap their PID 6 and retain their enrolled identifying data on smart card 54, while using other PIDs 6. This is the same process used in digital portable telephones today. A user can take the SIM card out of the telephone and swap phones without any security issues.

Verification is carried out when a user places his finger on platen 15, or presses a verify button if included in PID 6. In the embodiment illustrated in FIG. 4A, the verify button can be a dedicated button, such as the # button 55, or could be any other button or sequence of buttons. Each time the user places his or her finger on platen 15 (or presses the verify button and places their finger on platen 15) the optics unit 12 creates a fingerprint signal indicative of the fingerprint image of the user's finger on platen 15. The fingerprint signal is compared to the stored fingerprint template. If the two are significantly similar, the user's identity is verified to be the enrolled person. Verification takes about 1 second or less once the fingerprint template has been retrieved from storage. The user's fingerprint is always verified with the fingerprint template to allow the use of the encryption key.

In programmable PID's, verification for individual users can be set at various threshold levels to account for users who may have very fine, worn or

damaged fingers. In this event the ease of use can be enhanced by reducing their verification threshold. Verification threshold can be set at the time of enrollment.

Once the owner or person controlling the unit is enrolled, the unit can then be "registered" with numerous organizations. The host organization is only interested in knowing the ID code and the public encryption key.

The operation of security system 2 illustrated in FIG. 1 is different from the operation of security system 2A illustrated in FIG. 2. The operation of the embodiment illustrated in FIG. 1 will be described first.

In the first embodiment illustrated in FIG. 1, each of PID 6 and host facility 4 include transmit and receive functions. A communication from PID 6 to host system 30 is encrypted according to an encryption algorithm that employs a private key in encrypting and a public key to decrypt. The public encryption key is associated with PID 6 and therefore also with the enrolled person. The private encryption key is stored or loaded into PID 6 at registration time or at manufacture. When a user registers with each host system 30, the user provides the user's ID code and public key to host facility 4 as part of the user's account record. The public key can be stored by the host system. Alternatively, the user provides the public key to a central authority (trusted third party 39) with which host system 30 can communicate.

Referring now to FIG. 7, a user of PID 6 approaches host facility 4, e.g., an ATM (100). As PID 6 reaches the range of the host facility's receiver module 38, the microprocessor is "powered up." The user may have to select a transmission mode that matches that of host system 30, if more than one transmission mode is available on PID 6. Processor circuit 18 causes transmitter module 28 to transmit the ID code signal without encryption (102). This is received by host receiver module 38 and passed on to host processing unit 32 (104). Host processing unit 32 verifies that the received ID code signal represents a registered ID code (106). If the verification fails, then the access process ends (108). If the ID code is verified, then the account or user information is located, including the public encryption key associated with the registered ID code (110). The public encryption key may have to be retrieved from a remote source, such as a central authority. A large random number is also generated by host processing

unit 32 (112), and is passed on to transmitter module 40. Transmitter module 40 transmits a random number signal indicative of the random number to PID 6 (114). Receiver module 26 passes the random number signal to processing unit 16 (116). PID 6 performs a user verification (118). If the verification fails, the process ends (108). Alternatively, PID 6 can display a prompt to try again. If the user's identity is successfully verified as a match with the enrolled person based upon a comparison of the stored fingerprint template and a fingerprint image signal generated when the user places his finger on platen 15, the private encryption key associated with PID 6 is used to encrypt the random number according to an encryption algorithm (120). Processing unit 16 causes transmitter module 28 to transmit a signal representing the encrypted random number to host system 30 (122), where host processing unit 32 uses the public encryption key to decrypt the encrypted random number (124). Host processing unit 32 then determines if the decrypted random number matches the random number (126). If this is successful, then the user is granted access to the host facility (128). If this verification fails, the user is denied access (108). The step of verifying the identity of the user with the biometrics (118) can be performed at other junctures of the process, such as prior to transmitting the ID code signal (102), however, it must be carried out before encrypting the random number (120).

Hardware for host system 30 can include a small communication unit 8 with a sensor, such as an RF antenna. Processor circuit 34 can include a CPU to generate a random number, to verify the ID code received from PID 6, to decrypt the encrypted random number received from PID 6, and to compare the decrypted random number with the earlier generated random number.

As these transmissions are random, there is no possibility of scanning or tracking the codes other than to find the original ID code, which is effectively of no real use. The random number generators are such that they will always produce unique codes.

If a host system 30, such as a bank, a store, or a credit card company, implements this system, it would have the users register by presenting themselves with their PID 6 and the required personal identification papers, which is no different than current methods of obtaining a bank card to access accounts with an

ATM. The bank or other host system 30 would ask the user to complete a verify on their PID 6 and read the ID code and test the send and receive of the encryption codes. This would establish the public key with the bank and confirm the private key in PID 6. The user is now ready to use the system. Note that the bank does not have the user's fingerprint template--it only has the ID code and the public encryption key. Therefore there is no privacy issue regarding release of the user's fingerprint template.

After the user registers, verification is as described above. From the bank's point of view, the ATM (for example) commences normal operation. The user, instead of entering a bank card and a personal identification number (PIN), may simply press a verify pad or button on their PID 6 while placing their finger on platen 15. The ATM receiver reads the ID code, and if the code is valid generates a large random number, and transmits the number to the user's PID 6. If the validation is successful, PID 6 then encrypts the random number using the private encryption key according to the encryption algorithm, and transmits the result back. The bank system checks the result using the public encryption key and confirms the correct identity of the user. The transaction proceeds.

The bank's ATM will typically be connected to the Bank central system via network 42. Network 42 can be used for transmitting signals between the ATM and the bank central system where the CPU and data bases may be located.

The private encryption key can only be used after a verify, host system 30 knows the ID is correct as the key is unique to that user. Therefore, only that user could be carrying the reader. The key may well be installed during manufacture but only released after the unit is loaded with a template.

In a second mode of operation, typically used in car alarm systems and the like, PID 6A is configured as shown in FIG. 2 to transmit, and host facility 4A is configured to only receive. Receiver module 38 is a standard automobile or garage door type of installation. There is no special adaptation other than the required alarm or immobilizer installation. These systems include a "learn" mode, which is used to program in the new system. In learning a registering person's PID 6A, the host system 4A learns the ID code, the synchronization counter timing, and the encryption key of that PID 6A. This process is essentially the same as the learning

process for many current model garage door openers, automobile security systems and the like.

Referring to FIG. 8, to obtain access to host facility 4A, the user activates PID 6A by placing a finger on platen 15. PID 6A performs a user verification from the internally stored fingerprint template (200). If the verify succeeds, processing unit 16A causes encoder 23A to generate an encrypted signal (202). If not successful, the process ends (204). The encrypted signal includes the unencrypted ID code of PID 6, encrypted synchronization counter information and unencrypted function button information. The encryption employs the encryption key resident in encoder 23A. Transmitter unit 28 then transmits the encrypted signal to host facility 4A (206). Host facility 4A than passes the encrypted signal to host processing unit 32A, which checks the ID code for a match with the ID code of a registered user (208). Typically, there will be only a small number of registered users for car lock and garage door systems, and each may have the same ID code and encryption key. If there is no match, then the process ends (204). If there is a match, host processing unit 4A retrieves the stored encryption key and decrypts the encrypted portion of the received encrypted signal (210). Host processing unit then verifies that the synchronization counter information in the decrypted signal matches stored synchronization counter information in memory 36 (212). If the synchronization counter information does not match the stored information, then the process ends (204). If the synchronization counter information matches the stored information, then the user is granted access to host facility 4A (214). The access granted is determined by the function button information contained in the encrypted signal.

In both embodiments, the PID unit can be set in a low power "StandBy" or "Off" function, or could be powered on by the action of pressing the platen.

There are a large number of alternative applications. For example, a hotel could employ the invention in a door lock security system. A hotel registrant would register his PID with the hotel. The hotel would identify the user's ID code to the lock on his room's door. A member of the hotel staff would carry a master PID which would configure the door to that PID and some other master PID for

hotel staff. There would be no need for a hard wired communications system to each door unless central control is required.

The biometric sensor 11 may include a direct contact device instead of an optic sensor unit 12. Direct contact capacitive chip fingerprint sensors can be obtained from SGS Thomson Microelectronics, of Phoenix Arizona, from Veridicom, Inc., of Santa Clara California, and from Harris Semiconductor, of Melbourne, Florida. A direct contact thermal sensor may also be used for fingerprint sensing.

Other embodiments are within the scope of the claims.

For example, referring to FIGS. 10A and 10B, a PID 300 is configured to identify a user of a vehicle, provide immobilization security for the vehicle, and to automatically maintain a log of vehicle travel information. PID 300 is configured as a hand-held device with a finger platen 301, a display 302, an input keypad 304, and an input/output port 306. Input/output port 306 plugs into an in-vehicle adaptor module 307 which couples PID 300 to the vehicle power system 308, the engine management computer 310 and a global positioning system (GPS) 312. Adaptor module 307 includes a unique identification number that relates to the registration details of the vehicle. To operate the vehicle, the user must first be enrolled in PID 300 and PID 300 must be inserted into adaptor module 307. To start the vehicle, the user must activate a start-up option on PID 300 and must press (or swipe) a finger against finger platen 301. PID 300 extracts a representation of the user's fingerprint and compares the extracted information with a stored representation of the user's fingerprint. If the two fingerprint representations substantially match, PID 300 transmits a verification signal that enables the user to access the engine management system and operate the vehicle. After the user's identity has been verified, PID 300 begins to log trip information, including start time, vehicle location and trip log (map) information based on information received from GPS 312, vehicle speed and distance traveled. There is no need for the user to log travel information because all logging information is automated. The user may, however, enter additional information into PID 300 through keypad 304. PID 300 is programmable. For example, PID 300 may be programmed to prompt the user to enter additional identification information at

different times during a trip or at preselected vehicle locations based upon signals received from GPS 312. PID 300 includes a transceiver (e.g., an RF transceiver or a digital cellular telephone transceiver) that enables the device to be interrogated remotely (e.g., by devices located at preselected vehicle checkpoint locations, such as the locations of existing highway monitoring cameras).

Referring to FIG. 11, in another embodiment, a PID 320 is configured as a pocket-sized unit which may be clipped to a pocket 321 of a user's shirt and is configured to provide access to a secure location. The housing of PID 320 includes a pocket for holding a user identification card 325 (e.g., a photo ID card). PID 320 includes a finger platen 322, a notification light 324 (e.g., a red light emitting diode), a processor, and a receiver. When the receiver is located near (e.g., within about 0.5 meters) the transmitter of a host system which controls access to the secure location, the processor switches from a low power operation (standby or off mode) to a normal power operation and causes notification light 324 to flash, prompting the user to press (or swipe) a finger against finger platen 322. PID 320 extracts a representation of the user's fingerprint and compares the extracted information with a stored representation of the user's fingerprint. If the two fingerprint representations are sufficiently close, PID 320 transmits a verification signal to the host system. Upon receipt of the verification signal, the host system grants access to the secure location and logs information relating to the user and time access was granted. PID 320 includes an RF transceiver which enables PID 320 to wirelessly receive enrollment information (e.g., add or remove users) and to set access codes for each of the enrolled users.

Still other embodiments are within the scope of the claims.

WHAT IS CLAIMED IS:

1. A portable, hand-held personal identification device for providing secure access to a host facility, comprising:

a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative thereof;

a processing unit responsive to the biometric signal, being adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person, and to provide a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person, wherein the verification signal is indicative of the enrolled person or the device; and

a communication unit, including a transmitter circuit, is adapted to transmit the verification signal to a remote host system.

2. The personal identification device of claim 1, wherein the biometric sensor system includes a fingerprint sensor.

3. The personal identification device of claim 2, wherein the fingerprint sensor includes a platen adapted for placing a finger thereon.

4. The personal identification device of claim 3, wherein the fingerprint sensor further includes an optical image sensor.

5. The personal identification device of claim 1, wherein the biometric sensor system includes an optical image sensor.

6. The personal identification device of claim 5, wherein the optical image sensor comprises a CMOS chip.

7. The personal identification device of claim 1, wherein the processing unit includes a processor circuit, a memory and an encoder, wherein the memory stores the biometric data, and wherein the verification signal comprises an encrypted signal encrypted by the encoder.

8. The personal identification device of claim 7, wherein the encoder comprises an encoding circuit, and wherein the verification signal further comprises an ID code indicative of the enrolled person or the device.

9. The personal identification device of claim 7, wherein the encoder comprises an encryption algorithm programmed into the processor, and wherein the encryption algorithm employs a private key indicative of the enrolled person or the device.

10. The personal identification device of claim 9, wherein the communication unit further comprises a receiver circuit, wherein the memory further stores an ID code indicative of the enrolled person or the device, wherein the processor unit is further adapted to first cause the transmitter circuit to transmit an ID code signal indicative of the ID code to the host system, wherein the receiver circuit is adapted to receive a host response signal transmitted by the host system in response to the ID code signal, and wherein the processor unit employs the encryption algorithm and the private key to encrypt the host response signal to create the verification signal, and causes the transmitter circuit to transmit the verification signal to the host system only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person.

11. The personal identification device of claim 7, wherein the memory is located in a removable plug-in module, the personal identification device further comprising a socket adapted to receive the module.

12. The personal identification device of claim 1, wherein the communication unit further includes a receiving circuit being adapted to receive a host response signal from the host system.

13. The personal identification device of claim 1, wherein the communication unit is adapted for remote communication with the host system via a wireless communication medium.

14. The personal identification device of claim 1, further comprising a display.

15. The personal identification device of claim 14, further comprising a keypad.

16. The personal identification device of claim 1,

wherein the biometric sensor system includes a fingerprint sensor and wherein the biometric trait is a fingerprint;

wherein the communication unit further comprises a receiver circuit adapted to receive signals transmitted by the host system;

wherein the processing unit includes:

memory for storing an ID code associated only with the device, a personal encryption key associated only with the device, and the biometric data;

a processor circuit adapted to encrypt the host response signal according to an encryption algorithm employing the personal encryption key;

wherein the processing unit is further adapted to first cause the transmitter circuit to transmit an ID code signal indicative of the ID code to the host system, wherein the receiver circuit is adapted to receive a host response signal transmitted by the host system in response to the ID code signal, and to employ the encryption algorithm and the private encryption key to create the verification signal by encrypting a host response signal received by the receiver circuit from the host system in response to the ID code signal.

17. The personal identification device of claim 16, wherein the memory is located in a removable plug-in module, the personal identification device further comprising a socket adapted to receive the module.

18. A portable, hand-held personal identification device for providing secure access to a host facility, comprising:

a housing;

a fingerprint sensor system capable of sensing a fingerprint of a user and providing a fingerprint signal indicative thereof, the fingerprint sensor system including a platen on a surface of the housing adapted to receive a finger;

a communication unit in the housing being adapted for wireless communication with a separate host system, including a transmitting circuit and a receiving circuit; and

a slot in the housing for receiving a smart card that includes a memory.

19. The personal identification device of claim 18, in combination with the smart card, wherein the memory in the smart card stores a fingerprint template representative of the fingerprint of an enrolled person, and an ID code and a personal encryption key being associated with the device, wherein the processing circuit is adapted to cause the ID code signal from memory to be transmitted by the transmitting circuit, and wherein the processing circuit is further adapted to cause a host response signal received by the receiving circuit signal from the host system in response to the ID code signal to be encrypted according an encryption algorithm employing the personal encryption key and to cause the encrypted host response signal to be transmitted by the transmitting circuit only if the fingerprint signal corresponds sufficiently to the fingerprint template to verify that the user is the registered person.

20. The personal identification device of claim 18, further comprising an alphanumeric display.

21. The personal identification device of claim 20, further comprising a keypad for inputting data.

22. A method of providing secure access to a host facility, comprising:

registering one or more persons with the host facility, including storing a unique ID code and a public encryption key for each registered person;

receiving a first transmission comprising a first user signal at the host facility;

generating and then transmitting a random number signal only if the first user signal represents one of the stored ID codes;

receiving a second transmission comprising a second user signal at the host facility;

decrypting the second user signal with the public encryption key associated with the registered person who is also associated with the stored ID code represented by the first user signal; and

providing access to the host facility only if the decrypted second user signal represents the random number.

23. A method of providing access to a secure host facility only to registered persons, comprising:

registering one or more registered persons with the host system, wherein registering each registered person includes storing an ID code associated only with a portable hand-held device under the control of that registered person;

transmitting an ID code signal from a portable hand-held device to a facility of the host system, wherein the ID code signal represents an ID code associated with the transmitting device;

generating, at the host facility, a random number signal representing a random number in response to the ID code signal only if the ID code signal is representative of the ID code of the device controlled by one of the registered persons;

retrieving, with the host system, a public key associated with the one of the registered persons only if the ID code signal is representative of the ID code of the one the device controlled by the one of the registered persons;

transmitting the random number signal from the host facility to the transmitting device;

receiving the random number signal with the transmitting device;

generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of the transmitting device;

comparing, with the transmitting device, the user fingerprint signal to a fingerprint template stored in the transmitting device, the fingerprint template representing a fingerprint image of a person who is enrolled with the transmitting device;

encrypting the random number signal with the transmitting device, the random number signal being encrypted according to an encryption algorithm employing a private key associated only with the transmitting device;

transmitting the encrypted random number signal from the transmitting device to the host facility only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person;

decrypting the encrypted random number signal with the host system, including employing the retrieved public key; and

providing the user access to the host facility only if the decrypted encrypted random number signal represents the random number.

24. The method of claim 23, wherein retrieving the public key includes retrieving the public key from a trusted third party.

25. The method of claim 23, wherein transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each includes transmitting via a wireless transmission.

26. The method of claim 23, wherein transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each includes transmitting via at least one of a modem, a cable access TV line, and a computer communication medium.

27. A method of providing a secure function at a host facility only to a registered person, comprising:

registering a person with the host facility by storing an ID code associated only with a portable registered device controlled by the registered person, learning a synchronization counter of the registered device, storing an encryption key associated with the registered device and associating the encryption key of the registered device with the stored ID code;

generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of a portable user device;

comparing, with the user device, the user fingerprint signal to a fingerprint template stored in the user device, the fingerprint template representing a fingerprint image of an enrolled person who is enrolled with the user device;

generating an access signal with the user device only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person, the access signal comprising an ID code associated only with the user device, button press information representing a requested function, and encrypted data encrypted with an encryption key associated with the user device, the encrypted data including a synchronization counter associated with the user device;

transmitting the access signal from the user device to the host facility;

determining, with the host facility, if the ID code in the access signal matches the stored ID code;

retrieving the encryption key of the registered device if the match is successful;

employing the encryption key of the registered device to decrypt the encrypted data and determine the synchronization counter of the user device;

comparing the synchronization counter of the user device with the synchronization counter of the registered device;

providing the requested function represented by the button press data only if the synchronization counter of the user device matches the synchronization counter of the registered device.

28. A method of accessing a secure host facility, comprising:

sensing a biometric trait of a user that is unique to a user with a biometric sensor system of a portable device, and providing a biometric signal indicative of the biometric trait;

comparing, with the portable device, the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person;

providing a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person; and

transmitting the verification signal and an ID code signal to a remote host system, wherein the ID code signal is indicative of an ID code associated only with the portable device, and wherein the host system provides access to the secure facility in response to the verification signal only if host facility determines that personal device associated with the ID code belongs to a registered person.

29. A personal identification system, comprising:

a biometric sensor configured to extract a representation of a biometric trait of a user;

a processor configured to verify the user's identity based upon a comparison of a representation of a biometric trait extracted from a user with a stored representation of the biometric trait; and

a transmitter configured to transmit a verification signal indicative of a successful verification of the user's identity.

30. The system of claim 29, wherein the processor is configured to process signals received from a global positioning system (GPS) receiver.

31. The system of claim 30, wherein the processor is configured to derive trip information from the signals received from the GPS receiver.

32. The system of claim 31, wherein the trip information includes the location of the GPS receiver.

33. The system of claim 32, wherein the processor is programmable to prompt the user for additional verification information when the GPS receiver is positioned at a particular location.

34. The system of claim 29, further comprising a user input configured to enable a user to enter trip information, and wherein the processor is configured to process information received from the user.

35. The system of claim 29, wherein the transmitter is further configured to transmit signals representative of stored trip information.

36. The system of claim 29, wherein the biometric sensor, the processor, and the transmitter are housed within a portable, hand-held housing.

37. The system of claim 36, further comprising an input device mounted inside a vehicle and coupled to the vehicle's power system, and wherein the input device is adapted to receive the verification signal from the transmitter and to enable the user to turn on the vehicle only upon receipt of the verification signal.

38. The system of claim 36, wherein the housing has the form of a pocket-sized security badge.

39. The system of claim 36, wherein the housing is configured to receive a graphical representation of the user.

40. The system of claim 29, further comprising an automatic door locking device coupled to a vehicle door and adapted to unlock the door upon receipt of the verification signal.

41. The system of claim 29, further comprising an automatic door locking device coupled to a vehicle trunk and adapted to unlock the trunk upon receipt of the verification signal.

42. The system of claim 29, further comprising a receiver, and wherein the processor is operable to switch the system from a low power operation to a normal power operation when the receiver receives a power-up signal from a host system.

43. The system of claim 29, further comprising a memory configured to store the representation of the biometric trait.

44. The system of claim 44, wherein the memory is housed within a portable housing separable from the biometric sensor, processor and transmitter.

45. The system of claim 29, wherein the biometric sensor is configured to extract a representation of the user's fingerprint.

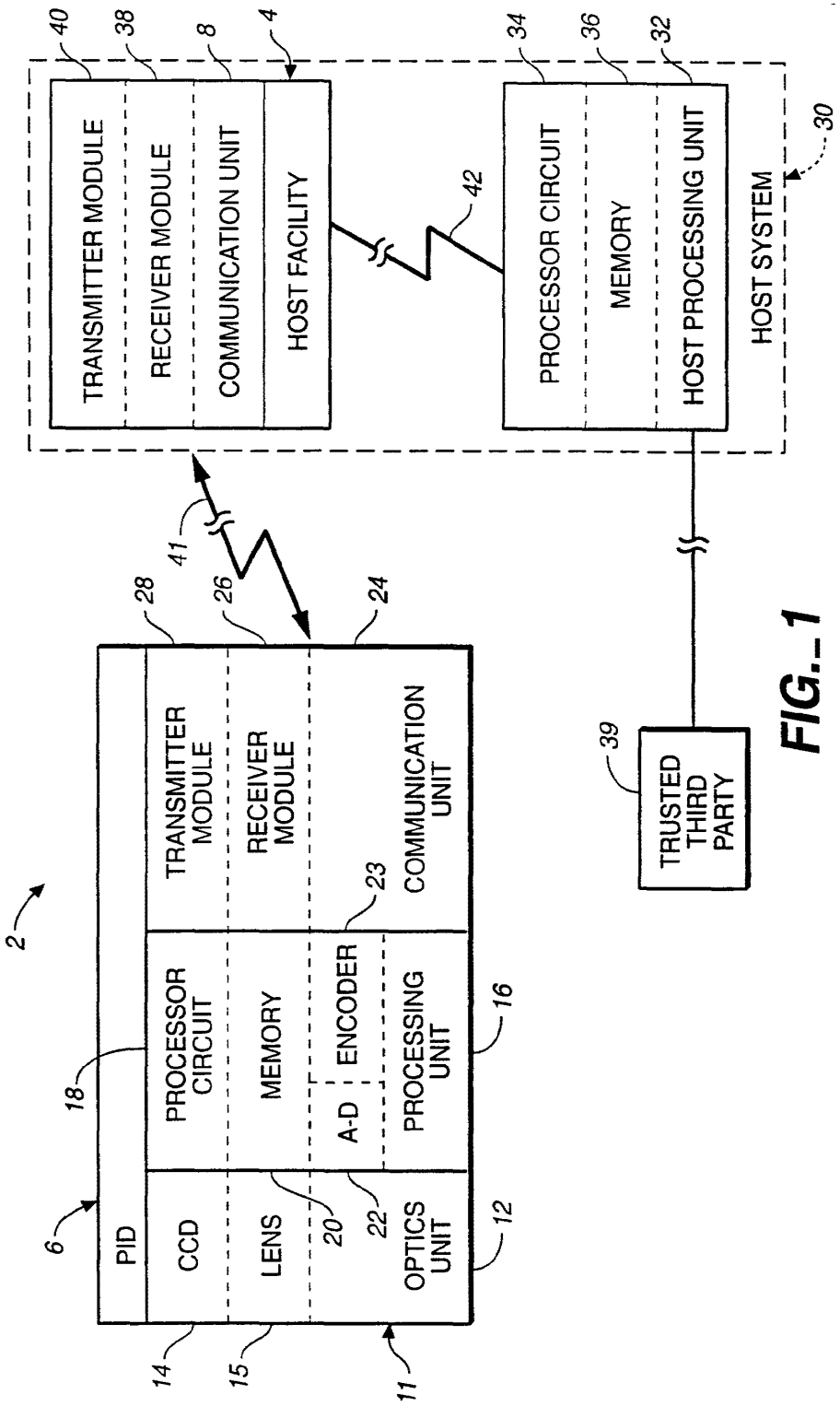


FIG._1

WAVELYNX EX. 1003, Pg. 1762
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

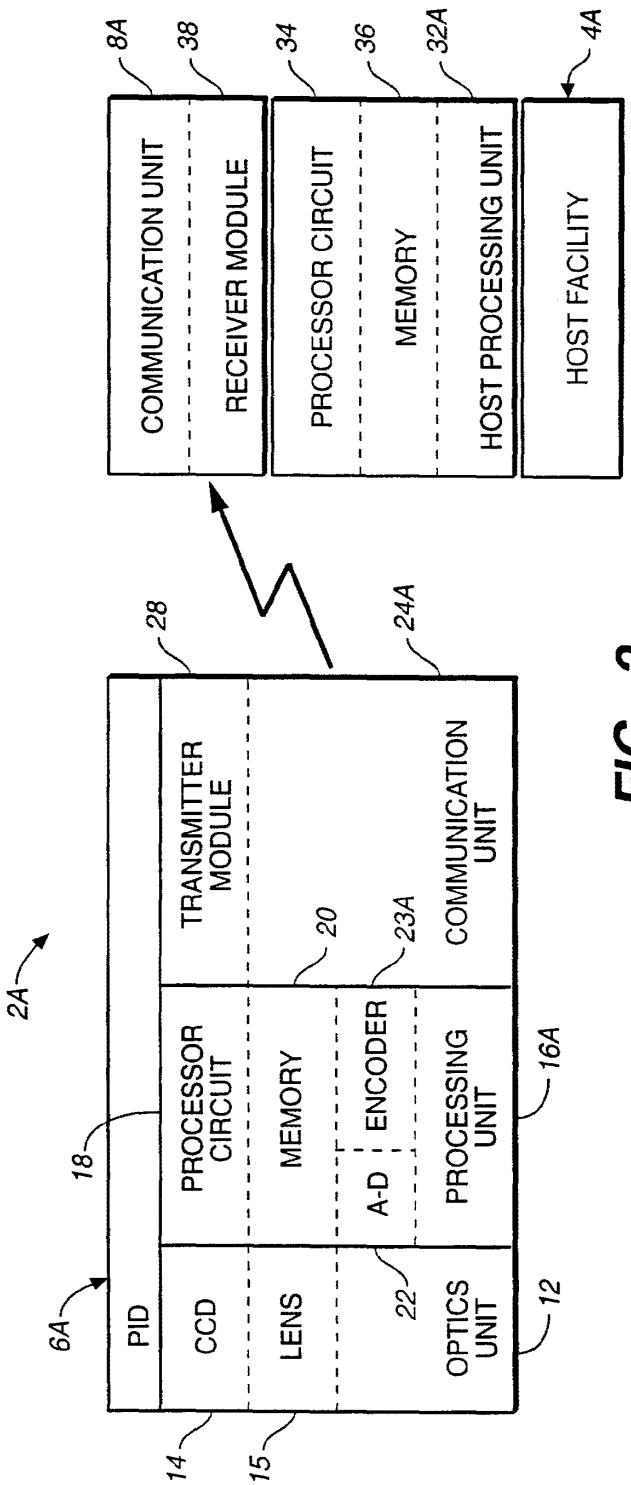


FIG._2

WAVELYNX EX. 1003, Pg. 1763
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

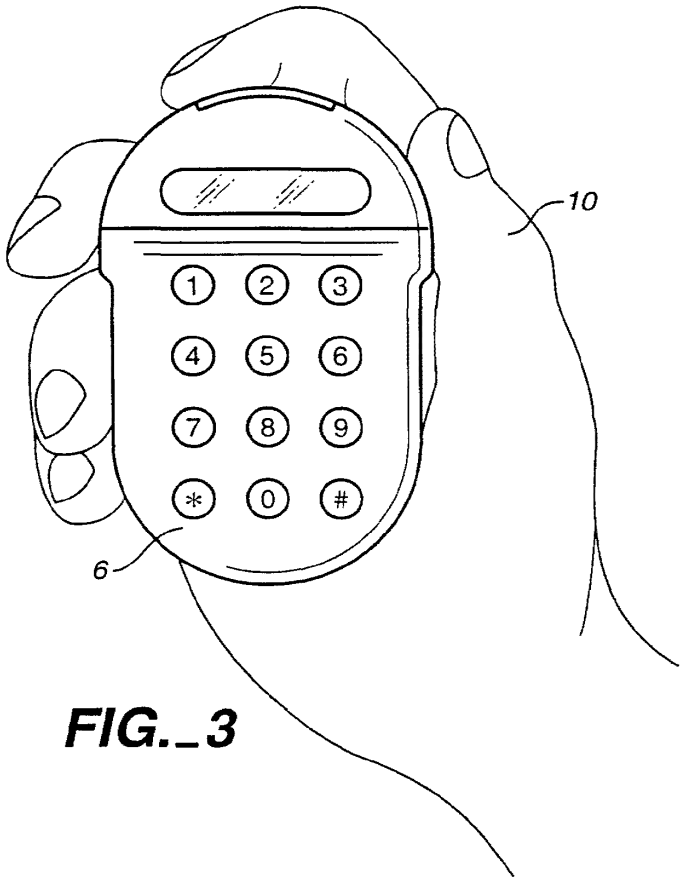


FIG._3

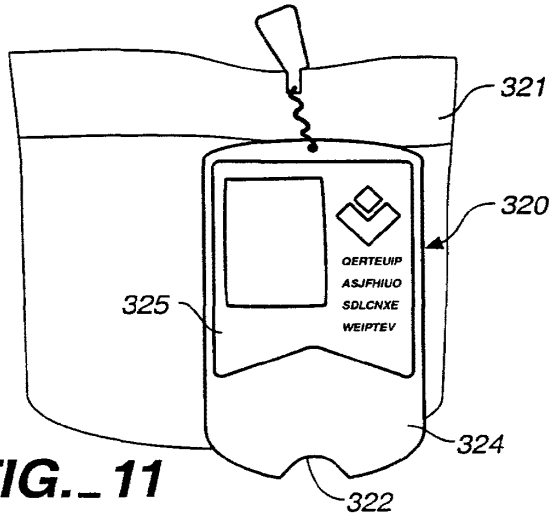


FIG._11

WAVELYNX EX. 1003, Pg. 1764
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

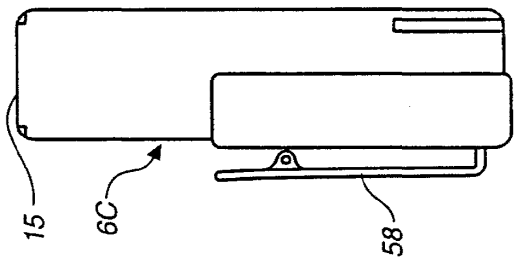


FIG._5B

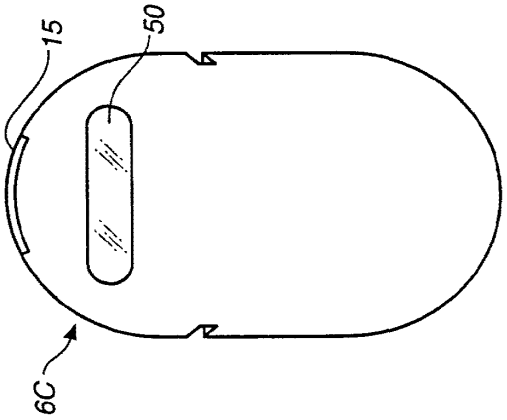


FIG._5A

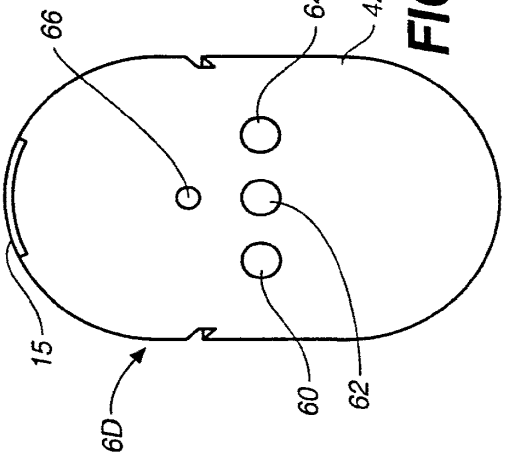


FIG._6

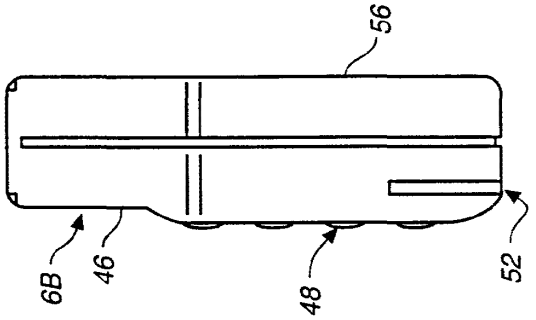


FIG._4B

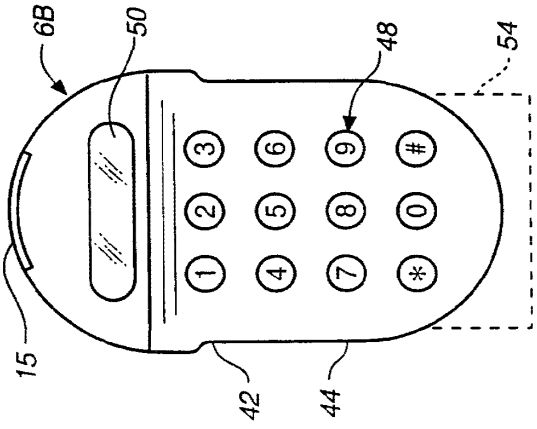


FIG._4A

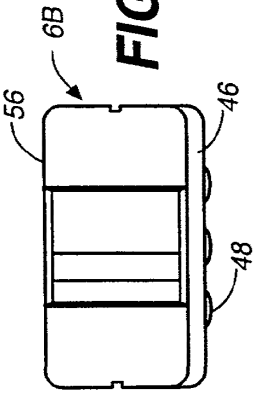


FIG._4C

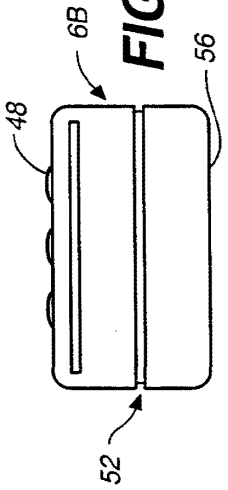


FIG._4D

WAVELYNX EX. 1003, Pg. 1765
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

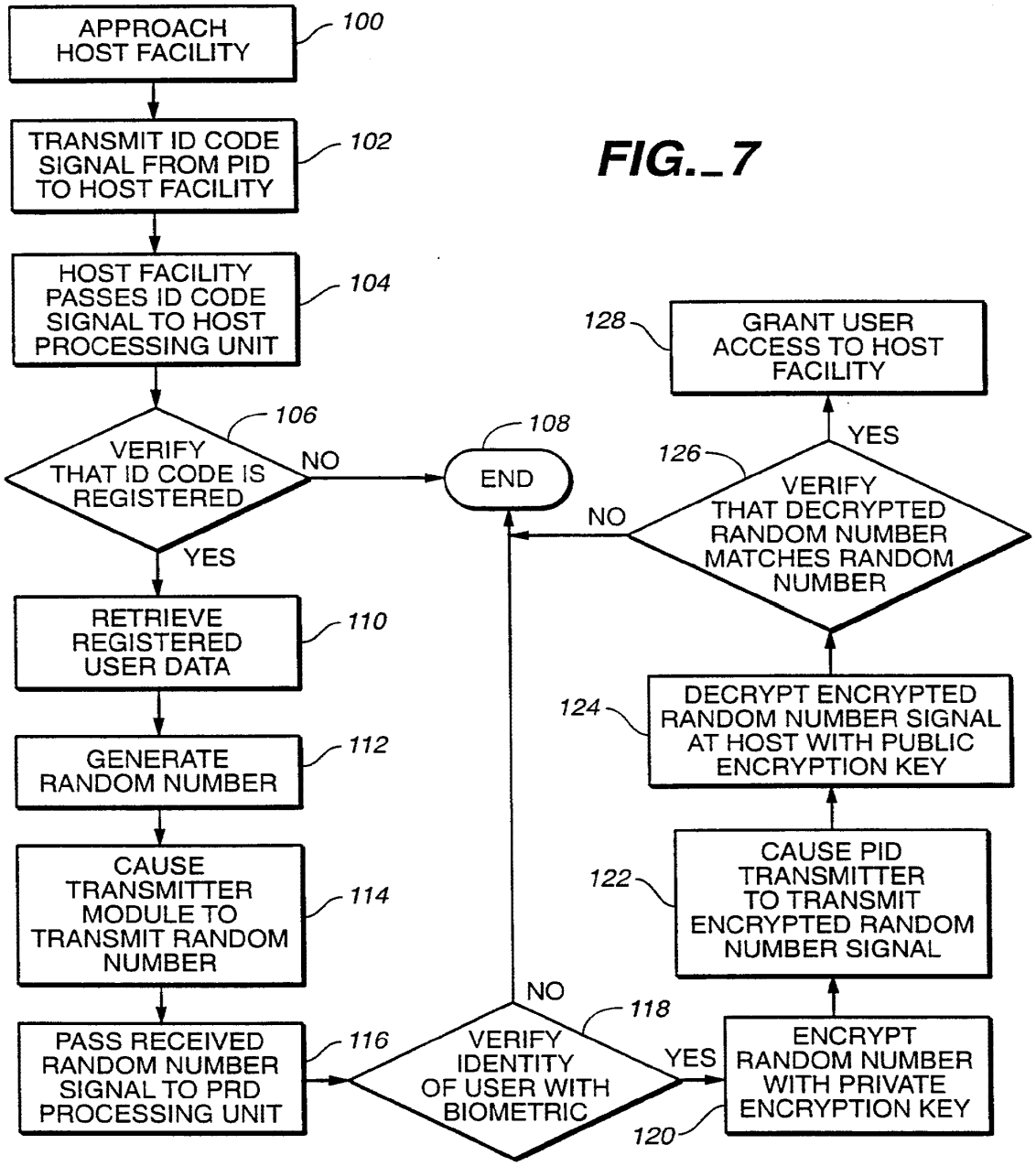


FIG._7

WAVELYNX EX. 1003, Pg. 1766
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

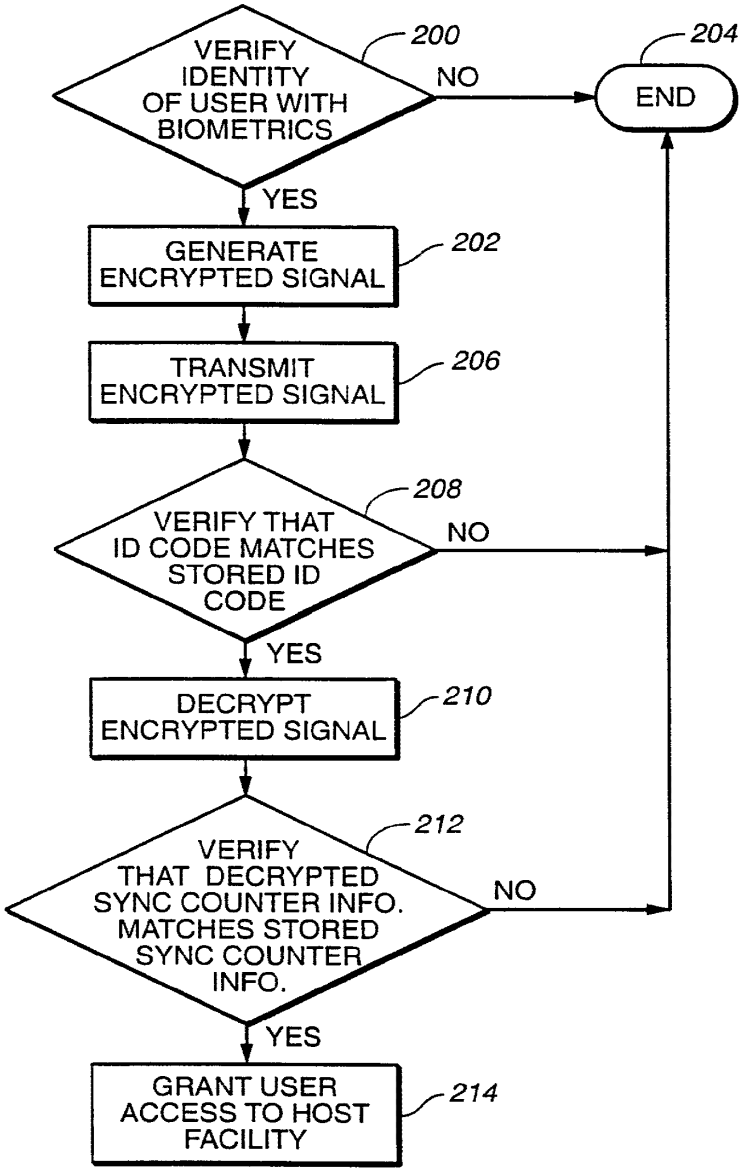


FIG._8

WAVELYNX EX. 1003, Pg. 1767
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

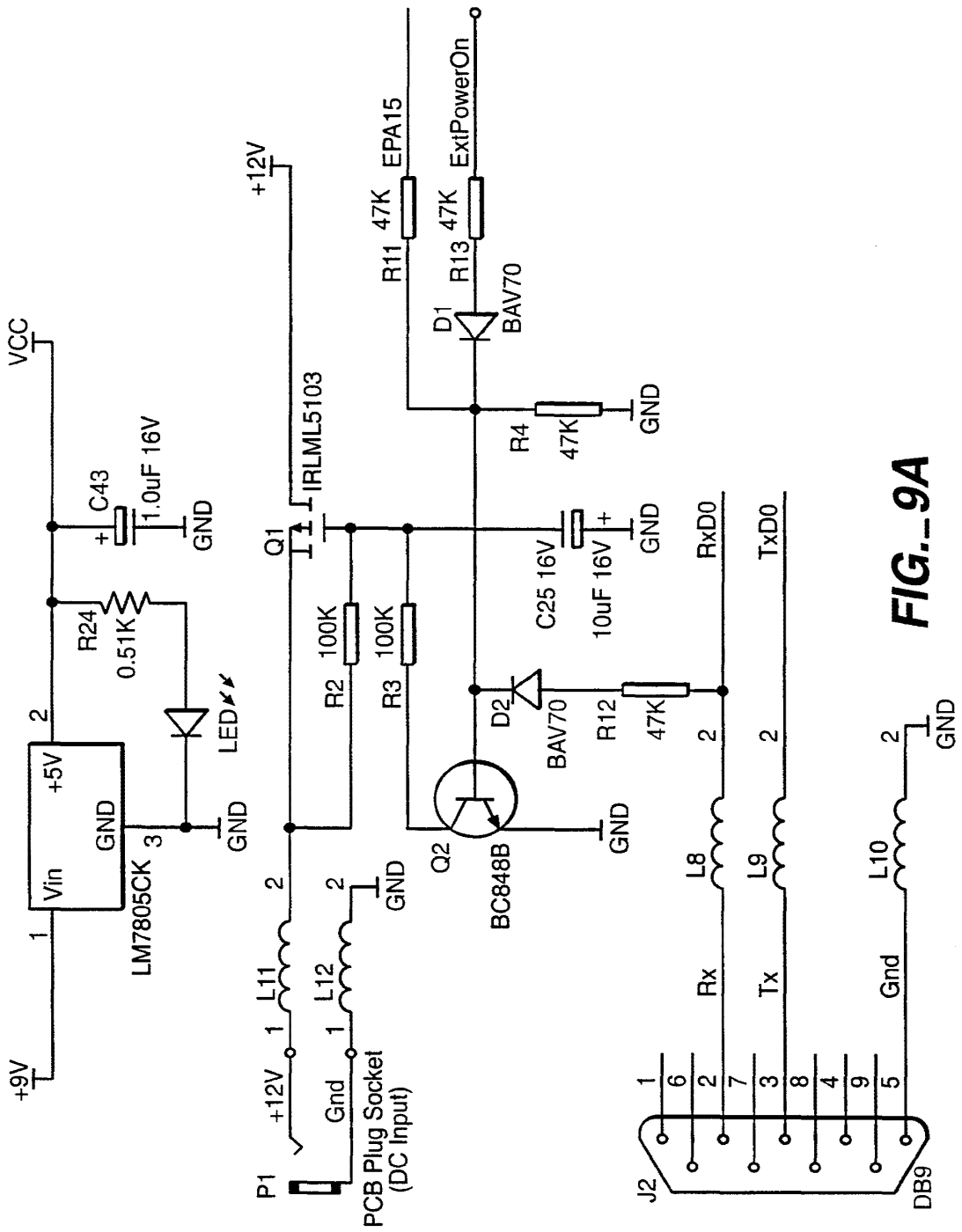


FIG._9A

WAVELYNX EX. 1003, Pg. 1768
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

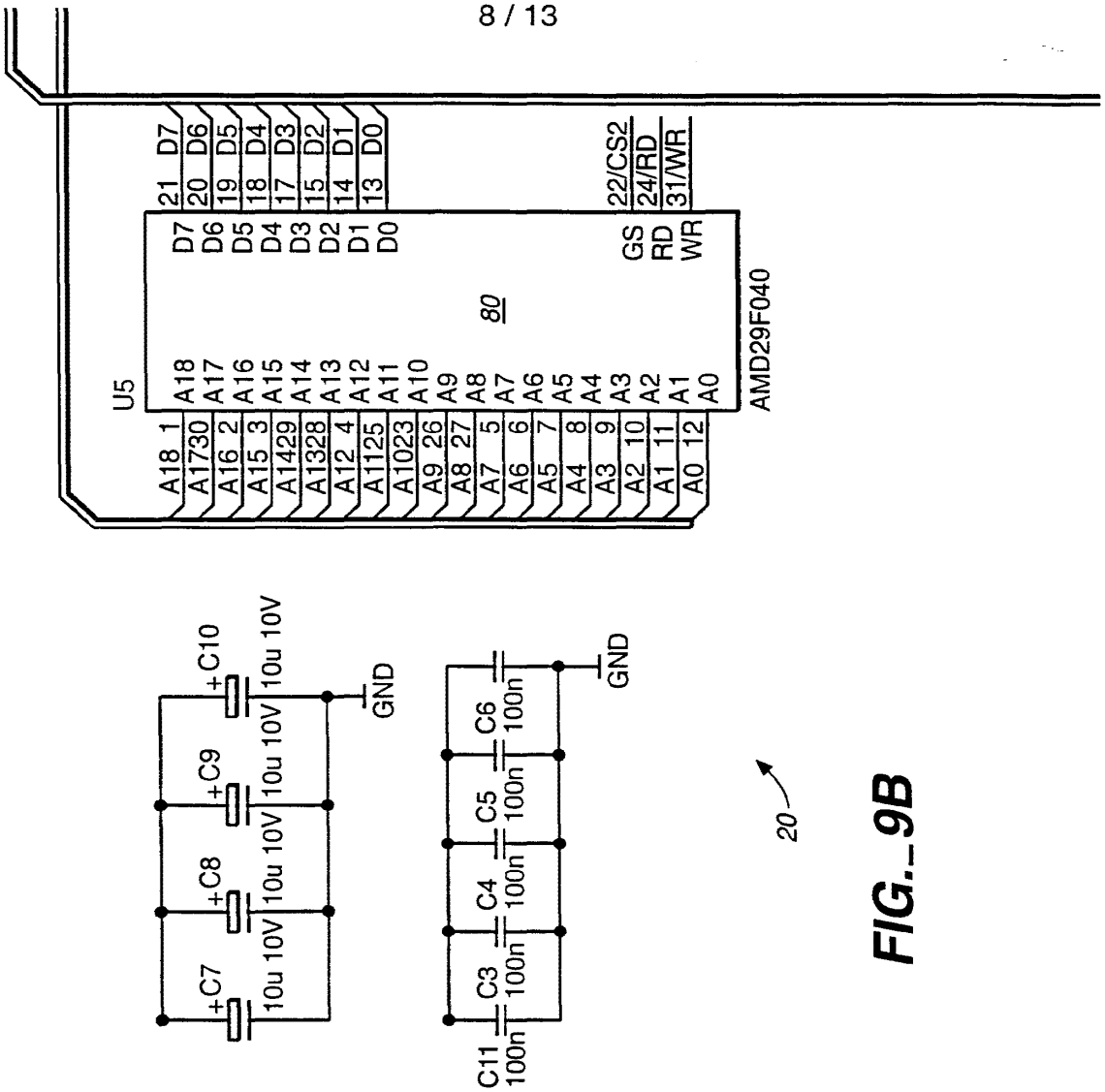


FIG._9B

WAVELYNX EX. 1003, Pg. 1769
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

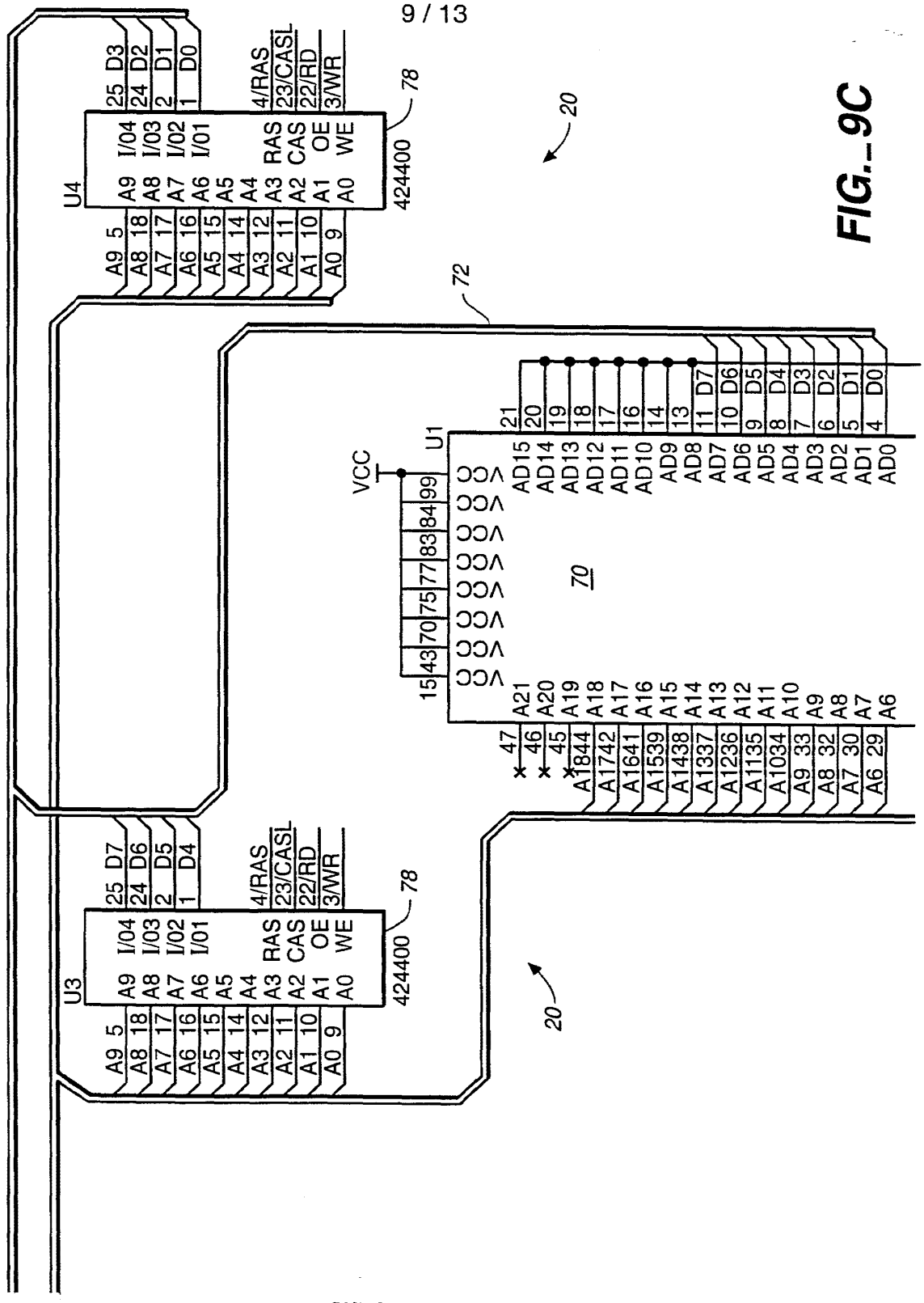


FIG._9C

WAVELYNX EX. 1003, Pg. 1770
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

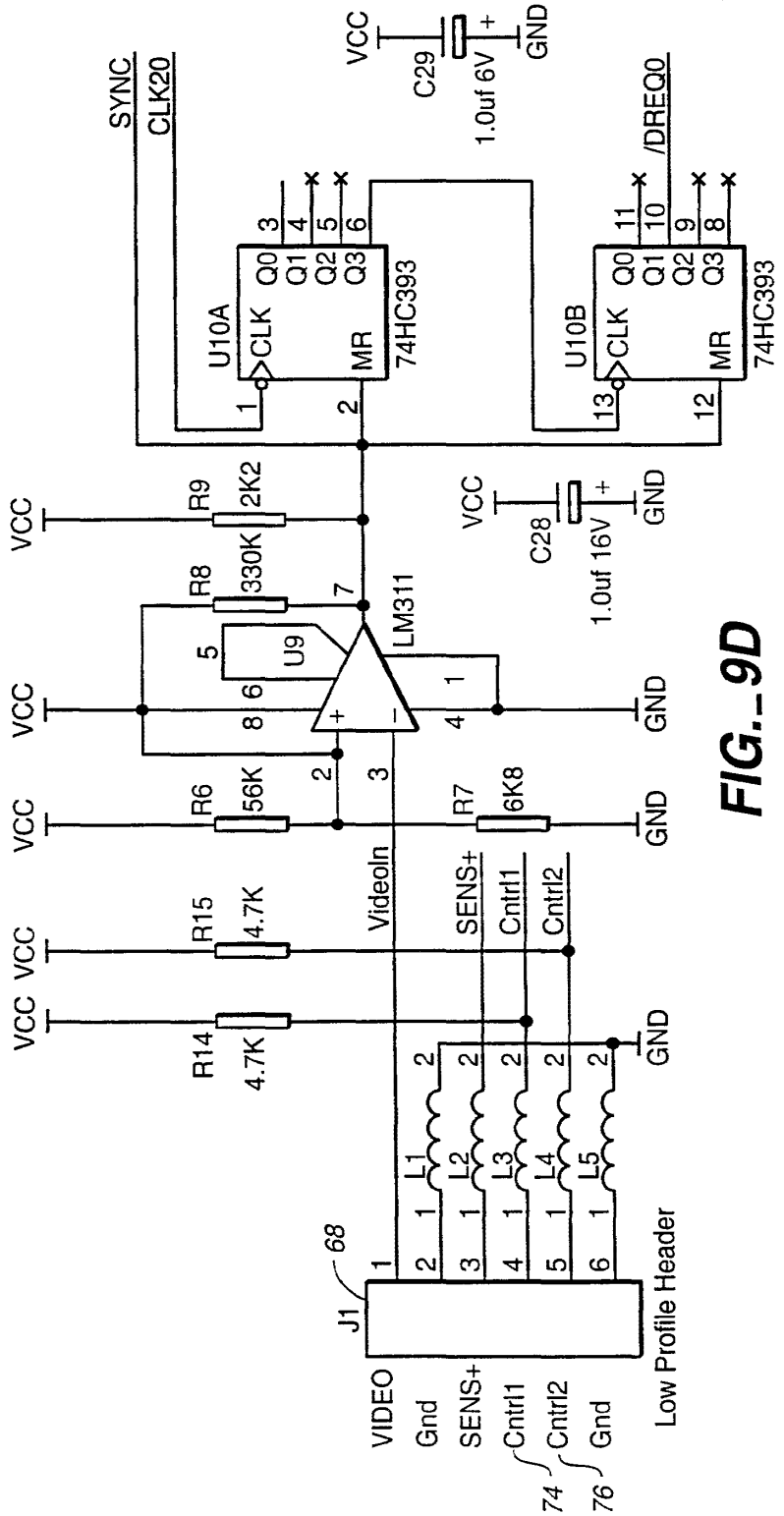


FIG._9D

FIG._9A	FIG._9B	FIG._9C
FIG._9D	FIG._9E	FIG._9F

FIG._9

WAVELYNX EX. 1003, Pg. 1771
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

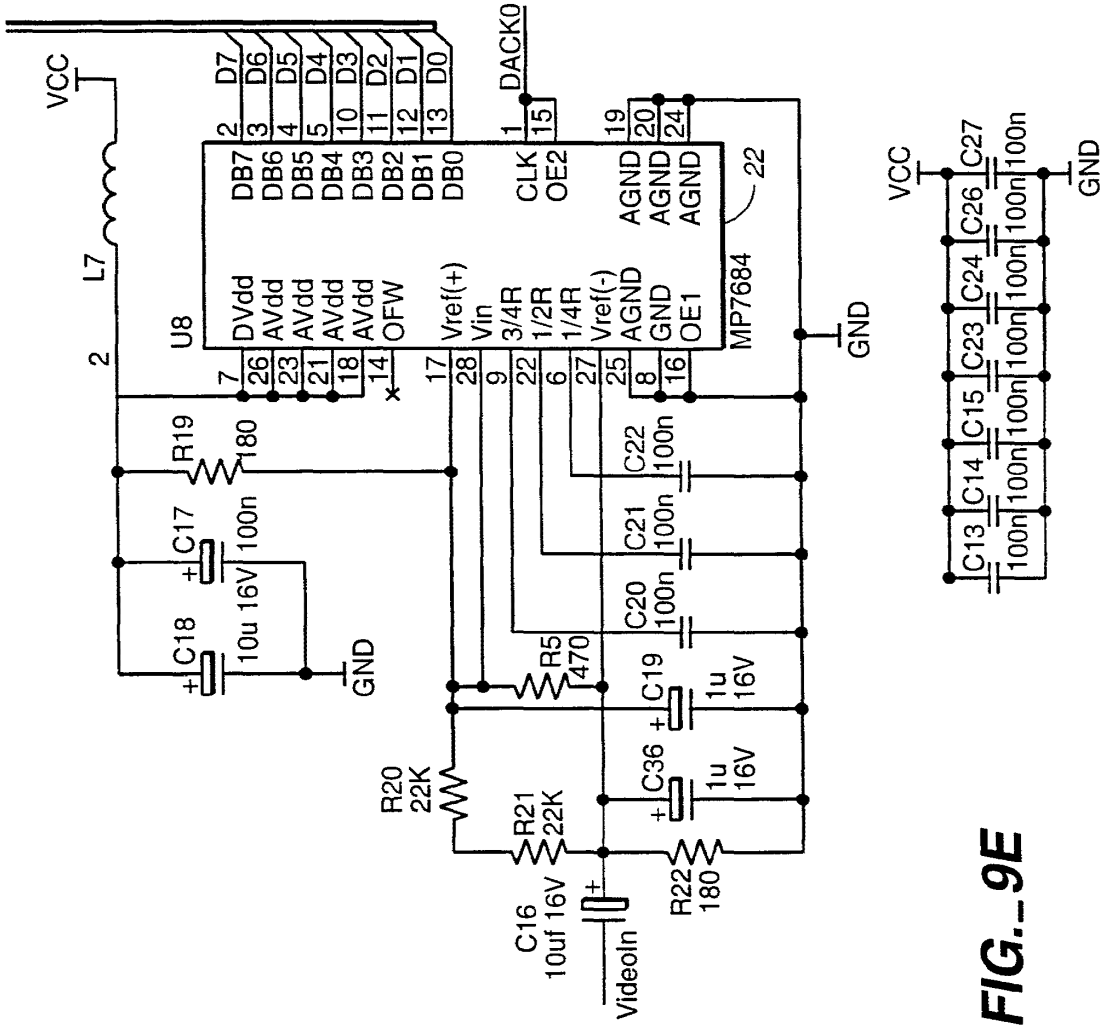
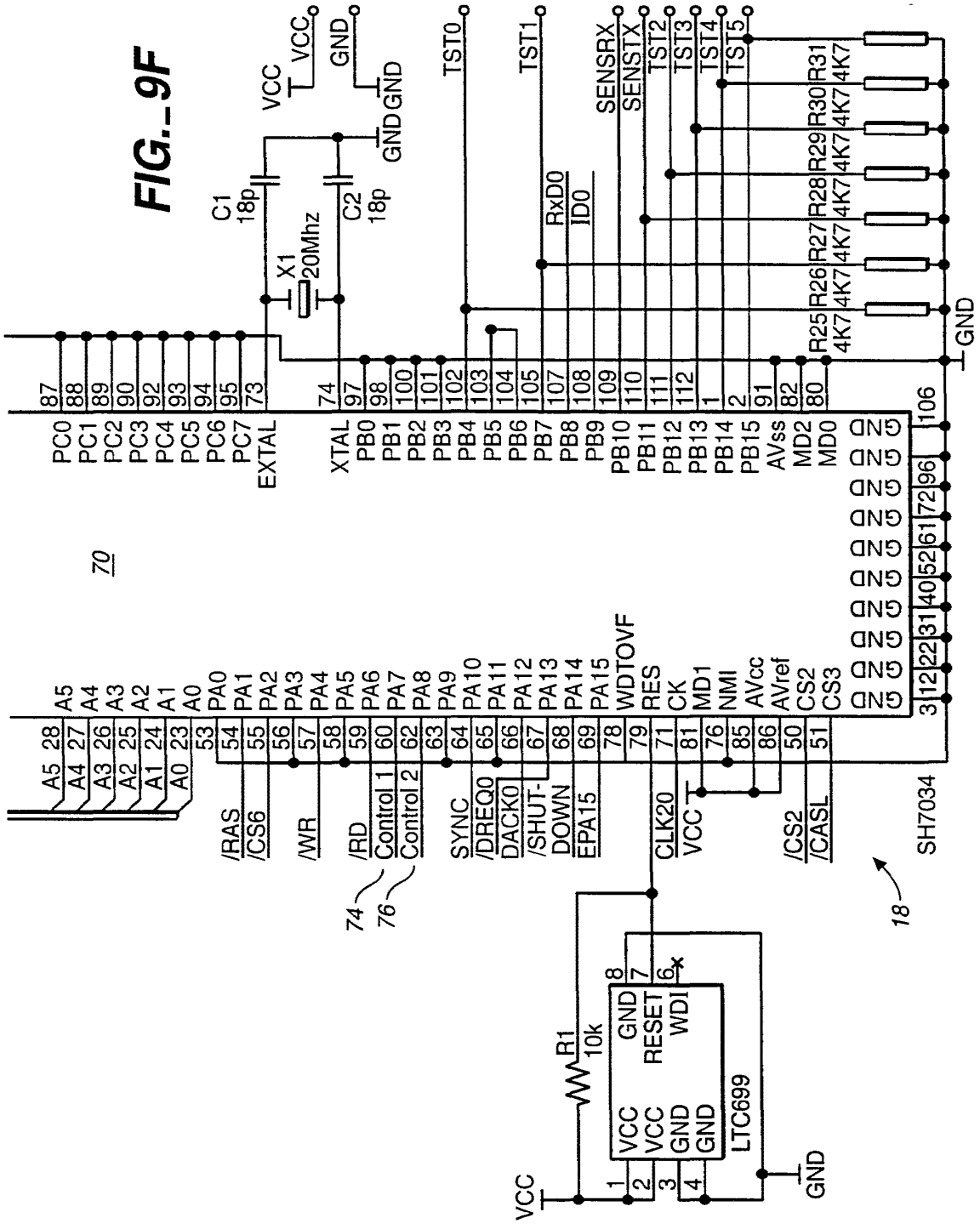


FIG._9E

WAVELYNX EX. 1003, Pg. 1772
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG._9F



SUBSTITUTE SHEET (RULE 26)

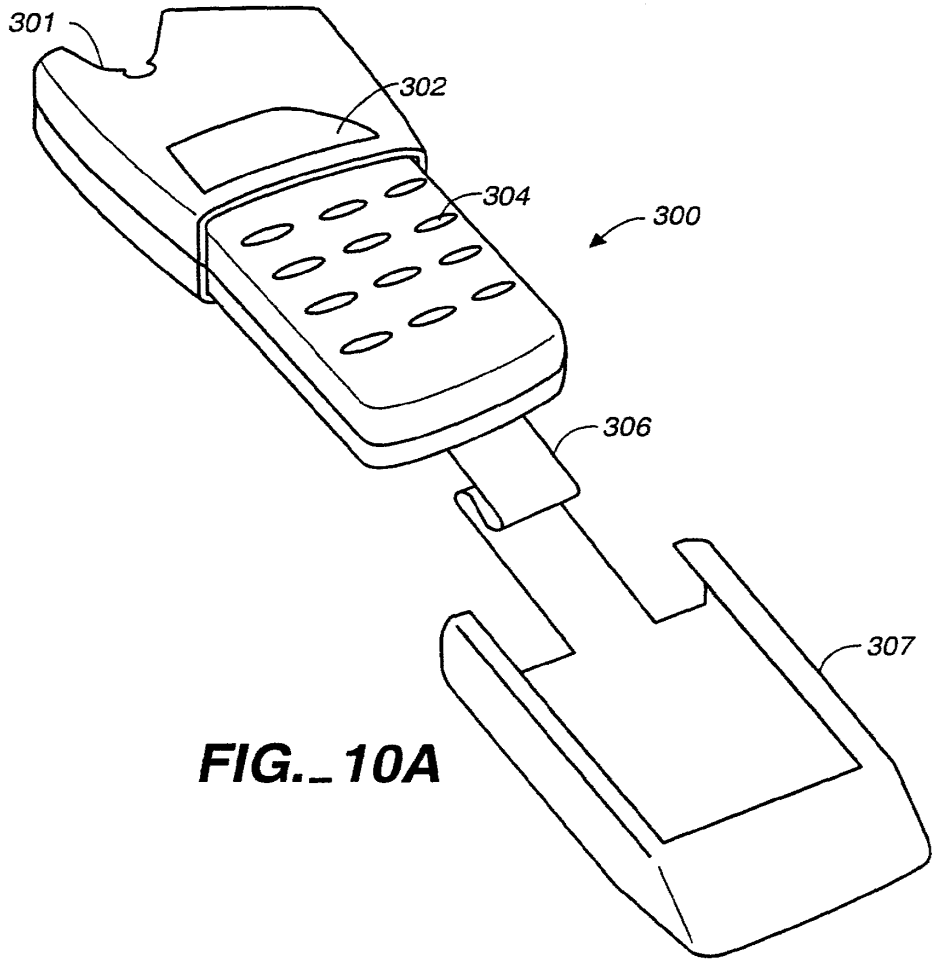


FIG._10A

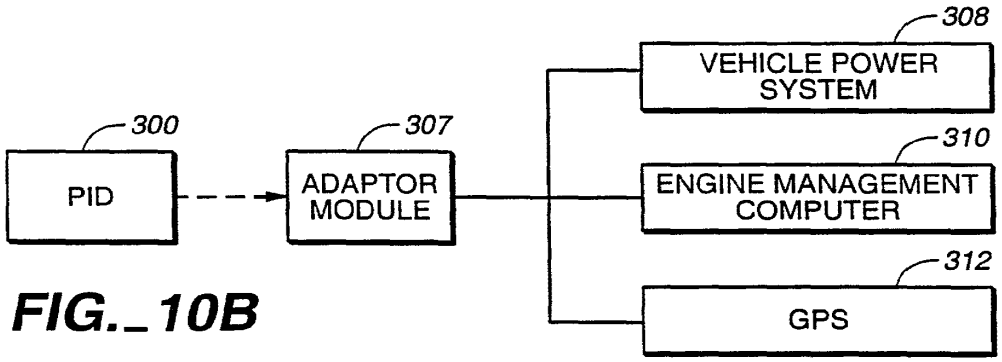


FIG._10B

WAVELYNX EX. 1003, Pg. 1774
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/08990

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00; H04Q 1/00
US CL :380/23; 382/115,116

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23; 382/115,116,125,126,127,313; 356/71; 340/825.34; 713/202

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,623,552 A (LANE) 22 April 1997, col.2, lines 29-35, col.3, lines 28-35,54-55, col.6, lines 42-44	1-2,13-14,29, --- 3-9,30-36, 38,40-41, 43,45
Y,E	US 5,903,225 A (SCHMITT et al) 11 May 1999, col.2, lines 53-60, col.4, lines 63-65,66-67, col.13, lines 40-65	3-9,30-36, 38,40-41, 43,45
A	US 5,546,471 A (MERJANIAN) 13 August 1996, col.2, lines 39-46, col.6, lines 48-54, col.11, lines 25-31.	3,4-5,25
A	US 4,995,086 A (LILLEY et al) 19 February 1991, col.2, lines 10-18, col.3, lines 10-15, col.4, lines 62-68	1-2,13,21

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
10 JUNE 1999	0 8 JUL 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-0040	Authorized officer GAIL HAYES Telephone No. (703) 305-0042

Form PCT/ISA/210 (second sheet)(July 1992) ★

WAVELYNX EX. 1003, Pg. 1775
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/08990

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

APS
search terms: biometric, fingerprint, finger print, thumb print, thumbprint, password, ID code, key, transmit, send, portable, device, wireless, authentication

Form PCT/ISA/210 (extra sheet)(July 1992) ★

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
22. Februar 2001 (22.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/13218 A1

(51) Internationale Patentklassifikation[7]: G06F 7/58, H04L 9/32 // G06F 7/72

(21) Internationales Aktenzeichen: PCT/DE00/02776

(22) Internationales Anmeldedatum:
16. August 2000 (16.08.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 39 059.2 18. August 1999 (18.08.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HESS, Erwin** [DE/DE]; Gottfried-Keller-Strasse 36, D-85521 Ottobrunn (DE). **SERF, Pascale** [DE/DE]; Max-Löw-Strasse 61, D-85579 Neubiberg (DE).

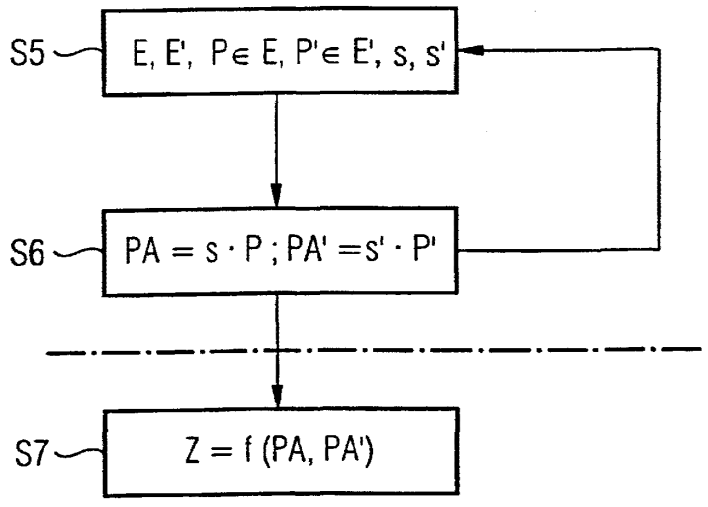
(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, D-80506 München (DE).

(81) Bestimmungsstaaten *(national)*: CA, JP, US.

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR GENERATING PSEUDO RANDOM NUMBERS AND METHOD FOR ELECTRONIC SIGNATURES

(54) Bezeichnung: VERFAHREN ZUM ERZEUGEN VON PSEUDOZUFALLSZAHLEN UND VERFAHREN FÜR ELEKTRONISCHE SIGNATUR



(57) Abstract: The invention relates to a method for generating pseudo random numbers and a method for electronic signatures. According to the inventive method for generating pseudo random numbers, points are determined on at least two different elliptical curves. A pseudo random number is produced respectively by linking the points. The linking of points of different elliptical curves to generate a pseudo random number makes it impossible to deduce the individual elliptical curves on the basis of the pseudo random numbers. The cryptographic security of the inventive method is thus tremendously increased because the computation of discrete logarithms is made impossible.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Erzeugen von Pseudozufallszahlen, sowie ein Verfahren für elektronische Signatur. Bei dem erfindungsgemäßen Verfahren zum Erzeugen von Pseudozufallszahlen werden Punkte auf zumindest zwei verschiedenen elliptischen Kurven bestimmt, und durch Verknüpfen der Punkte wird jeweils eine Pseudozufallszahl erzeugt. Das Verknüpfen der Punkte von unterschiedlichen elliptischen Kurven zu einer Pseudozufallszahl macht Rückschlüsse aus den so erzeugten Pseudozufallszahlen auf die einzelnen elliptischen Kurven unmöglich, wodurch die kryptographische Sicherheit des erfindungsgemäßen Verfahrens erheblich erhöht wird, weil die Berechnung diskreter Logarithmen unmöglich gemacht wird.

WO 01/13218 A1

WAVELYNX EX. 1003, Pg. 1777
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht:

— *Mit internationalem Recherchenbericht.*

— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

WAVELYNX EX. 1003, Pg. 1778
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Beschreibung

Verfahren zum Erzeugen von Pseudozufallszahlen und Verfahren für elektronische Signatur

Die Erfindung betrifft ein Verfahren zum Erzeugen von Pseudozufallszahlen und ein Verfahren für elektronische Signatur.

Zufallszahlen werden in der Kryptographie zum Verschlüsseln oder Signieren von Nachrichten benötigt. Im Artikel „Vom diplomatischen Code zur Falltürfunktion" von Otto Leiberich, Spektrum der Wissenschaft, Juni 1999, Seite 26 bis 34 wird ein Überblick über die Entwicklung der Kryptographie in Deutschland gegeben. Hierin ist ein früher verwendetes Wurm- oder Stromchiffrierverfahren beschrieben, bei dem eine sehr lange Zeichenfolge, die keinerlei innere Struktur aufweist, ein sogenannter Zeichenwurm oder Zeichenstrom, Zeichen für Zeichen zu einer zu verschlüsselnden Nachricht, dem Klartext, addiert wird. Sind es Buchstaben, werden sie zunächst nach dem Schema a = 0, b = 1, ..., z = 25 in Zahlen verwandelt. Damit keine größeren Zahlen als 25 entstehen, wird eine Addition modulo 26 durchgeführt. Im Zeitalter der Computer werden die Texte in binäre Zahlen verwandelt und Nullen und Einsen modulo 2 addiert. Der Empfänger subtrahiert vom empfangenen Geheimtext den Zeichenstrom - modulo 26 bzw. 2 - und gewinnt dadurch den Klartext zurück.

Der Zeichenstrom wird mit Hilfe von Zufallszahlengeneratoren erzeugt. Diese beruhten früher auf hochfrequenten Spannungsschwankungen bestimmter Röhren, sogenannter Thyratrons, und später auf radioaktiven Zerfallsereignissen.

Da jedoch die Zeichenströme jeweils parallel vom Sender zum Empfänger sicher übertragen werden müssen, ist ein erheblicher Durchsatz an sicherem Datentransfer notwendig.

Man hat deshalb Verfahren zum Erzeugen von Pseudozufallszahlen, sogenannte Pseudozufallszahlengeneratoren, entwikkelt, die in Abhängigkeit von einem Schlüssel eine im wesentlichen beliebig lange Folge von Pseudozufallszahlen erzeugen können. Hierdurch mußte bei obigem Codierverfahren lediglich ein Schlüssel zwischen den Kommunikationspartnern geheim übermittelt werden, was wesentlich einfacher handhabbar ist, als jeweils einen kompletten Zeichenstrom zu übermitteln.

Für heutige offene Netze, insbesondere das Internet, sind Verfahren entwickelt worden, bei denen zwei Kommunikationspartner, die zum ersten Mal miteinander kommunizieren wollen, sich verschlüsselte Nachrichten übersenden können. Diese Verfahren sind sogenannte asymmetrische Schlüsselverfahren, die auch als Public-Key-Verfahren bezeichnet werden, bei welchen der Empfänger seinen Schlüssel, den sogenannten Public Key, veröffentlicht.

Eines der bekanntesten Verfahren dieses Typs ist das sogenannte RSA-Verfahren, bei dem Teile der Schlüssel, die sogenannten Schlüsselmoduln, Produkte zweier großer Primzahlen sind. Der Sender der Nachricht kennt lediglich den Schlüsselmodul, also das Produkt, und kann mit diesem nach einer bestimmten mathematischen Funktion die Nachricht verschlüsseln. Zur Entschlüsselung der Nachricht genügt jedoch nicht die Kenntnis des Produktes, sondern man benötigt die beiden Primzahlen. Mit Hilfe dieser Primzahlen und einer entsprechenden Umkehrfunktion kann nur der richtige Empfänger, der den Schlüssel erzeugt hat, die verschlüsselte Nachricht entschlüsseln.

Die Zerlegung des Schlüsselmoduls in seine Teiler, die beiden Primzahlen, ist bei großen Moduln mit normalem Rechenaufwand praktisch nicht möglich. In „Faktorisierung großer Zahlen" von Johannes Buchmann, Spektrum der Wissenschaft, September 1996, Seite 80 - 88 ist das Problem der Zerlegung großer Zahlen in ihre Primzahlen ausführlich beschrieben und der Auf-

WAVELYNX EX. 1003, Pg. 1780
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

wand zur Zerlegung einer 129stelligen Zahl dargelegt. Diese Zahl wurde mit Hilfe von 600 Freiwilligen, die ihre Computer zur Verfügung gestellt haben, in die einzelnen Primzahlen zerlegt.

Nachteilig an dem RSA-Verfahren ist, daß es zu langsam für die Nachrichtenverschlüsselung ist, da zur Gewährleistung einer ausreichenden Sicherheit sehr große Zahlen - ungefähr 1000 Binär- oder 300 Dezimalstellen - verwendet werden müssen. Es sind derart große Zahlen mit anderen gleicher Größenordnung zu potenzieren, was zur Verschlüsselung von zu übertragenden Daten nicht schnell genug erfolgen kann. Das RSA-Verfahren wird deshalb lediglich zur verschlüsselten Übertragung von geheimzuhaltenden Schlüsseln für ein herkömmliches Verfahren verwendet, das dann die eigentliche Verschlüsselung vollzieht.

Als Alternative zu dem RSA-Verfahren sind Verfahren auf Grundlage von elliptischen Kurven entwickelt worden. Für die Kryptographie sind lediglich elliptische Kurven über endlichen Körpern relevant. Diese elliptischen Kurven über endlichen Körpern bilden Punktgruppen, in denen eine Addition und eine Multiplikation definiert sind, die mit der landläufigen Addition und Multiplikation nichts gemeinsam haben als die Rechenregeln. Die Multiplikation auf einer elliptischen Kurve über einem endlichen Körper ist eine Einwegfunktion, das heißt, daß die Umkehrung - die Berechnung sogenannter diskreter Logarithmen - im Normalfall rechentechnisch undurchführbar ist, wohingegen die Multiplikation sehr einfach und schnell ausgeführt werden kann. Diese Tatsache wird bei den auf elliptischen Kurven basierenden kryptographischen Verfahren ausgenutzt, indem der Empfänger sich eine Zufallszahl t wählt und auf Grundlage dieser Zufallszahl t und einer Multiplikation mit t auf der elliptischen Kurve einen Kurvenpunkt T bestimmt. Der Kurvenpunkt T wird als Schlüssel veröffentlicht, wohingegen die Zufallszahl t vom Empfänger geheimgehalten wird. Ein Sender kann mit Hilfe des Kurvenpunktes T

WAVELYNX EX. 1003, Pg. 1781
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

seine Nachricht verschlüsseln, die dann lediglich der Empfänger, der die dem Kurvenpunkt T zugrundeliegende Zufallszahl t kennt, entschlüsseln kann.

Solche auf elliptischen Kurven basierende Verfahren benötigen bei gleicher Sicherheit wie das RSA-Verfahren wesentlich weniger Rechenleistung. Derartige Verfahren können in Kleinstrechnern implementiert werden, wie z.B. in Chipkarten. Die Siemens AG vertreibt eine Chipkarte mit der Markenbezeichnung SLE44CR80S, in der ein Signaturverfahren auf der Basis elliptischer Kurven implementiert ist.

Zur Erzeugung der Schlüssel, des öffentlichen Schlüssels, den der Empfänger veröffentlicht, und seines entsprechenden privaten Schlüssels, werden wiederum Zufallszahlen benötigt.

Der Erfindung liegt deshalb die Aufgabe zugrunde, auf Basis elliptischer Kurven ein Verfahren zum Erzeugen von Pseudozufallszahlen zu schaffen, das einfach und schnell ausführbar ist und mit dem eine große Menge qualitativ hochwertiger Zufallszahlen erzeugt werden kann.

Diese Aufgabe wird durch ein Verfahren mit den Merkmalen des Anspruchs 1 gelöst.

Ferner liegt der Erfindung die Aufgabe zugrunde, ein Verfahren für elektronische Signatur auf Basis elliptischer Kurven sowie eine entsprechende Vorrichtung zu schaffen, die weniger Speicherplatz als bekannte Verfahren und Vorrichtungen für elektronische Signatur auf Grundlage elliptischer Kurven benötigen und auf kleinen Rechensystemen, insbesondere Chipkarten, implementiert werden können.

Die Aufgabe wird durch ein Verfahren mit den Merkmalen des Anspruchs 11 und eine Vorrichtung mit den Merkmalen des Anspruchs 12 gelöst.

WAVELYNX EX. 1003, Pg. 1782
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

Beim erfindungsgemäßen Verfahren nach Anspruch 1 zum Erzeugen von Pseudozufallszahlen werden Paare von Punkten bestimmt, die auf zumindest zwei unterschiedlichen elliptischen Kurven über einem endlichen Körper liegen, und in Abhängigkeit von jeweils einem solchen Paar von Punkten wird eine Zufallszahl ermittelt.

Da erfindungsgemäß zwei verschiedene elliptische Kurven benutzt werden, und die Pseudozufallszahl aus einem Paar von Punkten abgeleitet wird, wobei die beiden Punkte des Paares auf unterschiedlichen elliptischen Kurven liegen, ist es unmöglich, aus den derart ermittelten Pseudozufallszahlen auf die Kurvenpunkte zurückzuschließen. Bei Verwendung lediglich einer einzigen elliptischen Kurve zum Ableiten von Pseudozufallszahlen könnte durch Berechnen diskreter Logarithmen aus den Pseudozufallszahlen auf die Kurvenpunkte zurückgeschlossen werden. Hierdurch wäre es möglich, daß Dritte die Rechenregel der Pseudozufallszahlen bestimmen könnten und die weiteren Pseudozufallszahlen voraussagen könnten. Dies würde ein erhebliches Sicherheitsrisiko darstellen, das mit der vorliegenden Erfindung vermieden wird.

Das erfindungsgemäße Verfahren für elektronische Signatur kombiniert ein an sich bekanntes Signaturverfahren mit dem erfindungsgemäßen Verfahren zum Erzeugen von Pseudozufallszahlen. Die gleichen Routinen bzw. Einrichtungen können sowohl beim Signaturverfahren als auch bei der Erzeugung der Zufallszahlen verwendet werden, wodurch erheblich Programmcode und Speicherplatz eingespart werden kann. Zudem wirkt sich eine Optimierung der EC(=elliptic curve)-Arithmetik sowohl bei der Erzeugung der Pseudozufallszahlen als auch bei der unmittelbaren Ausführung des Signaturverfahrens vorteilhaft aus. Durch diese doppelte Verwendung der

WAVELYNX EX. 1003, Pg. 1783
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Routinen und Einrichtungen auf Basis elliptischer Kurven werden somit Synergieeffekte erzielt.

Ferner sind die erfindungsgemäß erzeugten Pseudozufallszahlen nicht von Zufallszahlen eines echten Zufallsgenerators zu unterscheiden und können mit relativ geringem Rechenaufwand erzeugt werden.

Die Erfindung wird nachfolgend beispielhaft anhand der Zeichnungen näher erläutert. In denen zeigen schematisch:

Fig. 1 eine elliptische Kurve über den reellen Zahlen,

Fig. 2 eine elliptische Kurve über einem endlichen Körper,

Fig. 3 die Addition zweier Punkte einer elliptischen Kurve über den reellen Zahlen,

Fig. 4 die Punkte der elliptischen Kurve $y^2=x^3+2x+9$ über dem Körper mod 13, die eine zyklische Gruppe mit 17 Punkten bilden,

Fig. 5 den Verfahrensablauf eines Ausführungsbeispiels der Erfindung in einem Flußdiagramm,

Fig. 6 das Grundprinzip des erfindungsgemäßen Verfahrens zum Erzeugen von Pseudozufallszahlen in einem Flußdiagramm, und

Fig. 7 den Aufbau eines Programmes zum Ausführen eines erfindungsgemäßen Signaturverfahrens.

Zunächst werden kurz die mathematischen Grundlagen zum Rechnen auf elliptischen Kurven erläutert. Eine elliptische Kurve E über einem Körper K ist eine Kurve, die durch eine kubische Gleichung der Form:

WAVELYNX EX. 1003, Pg. 1784
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

$y^2=x^3+ax+b$,

beschrieben werden kann mit a und b aus K, $4a^3+27b^2 \neq 0$. Paare (x, y) aus K x K, welche die Gleichung erfüllen, sowie das formale Paar (∞,∞) nennt man Punkte der Kurve E über K.

Eine elliptische Kurve über den reellen Zahlen ist in Fig. 1 gezeigt. Man beachte, daß elliptische Kurven keine Ellipsen sind.

Fig. 2 zeigt eine elliptische Kurve über einem endlichen Körper. Der algebraische Begriff Körper definiert einen „Zahlenbereich", in dem man nach den von den rationalen Zahlen bekannten formalen Rechenregeln addieren, subtrahieren, multiplizieren und dividieren kann. Es gibt unendliche Körper, wie z.B. die rationalen Zahlen, die reellen Zahlen, die komplexen Zahlen, und endliche Körper. Endliche Körper sind z.B. der Körper GF(p) der Zahlen mod p, wobei p eine Primzahl ist, bzw. der Körper $GF(2^n)$ der Binärvektoren der Länge n. („GF" steht für „Galois field", was ein Synonym für „endlicher Körper" ist.) Für die Kryptographie sind nur elliptische Kurven über endlichen Körpern relevant.

Fig. 3 zeigt die Addition zweier Punkte P_1, P_2 auf einer elliptischen Kurve über den reellen Zahlen, wobei sich der Punkt P_3 ergibt. Bei dieser Addition wird die Verbindungsgerade der Punkte P_1 und P_2 gebildet und deren 3. Schnittpunkt mit der elliptischen Kurve ermittelt. Dieser Schnittpunkt wird an der x-Achse gespiegelt und ergibt das Resultat P_3 der Addition von P_1 und P_2.

Diese Addition der Punkte auf elliptischen Kurven kann durch folgende Formeln ausgedrückt werden:

$x_3=r^2-x_1-x_2$, $y_3=r(x_1-x_3)-y_1$ mit
$r=(y_2-y_1)/(x_2-x_1)$, falls $x_1 \neq x_2$
$r=(3x_1^2+a)/2y_1$, falls $P_1=P_2$

wobei x_i, y_i die Koordinaten des Punktes P_i (i=1,2,3) sind.

Diese Formeln gelten auch für elliptische Kurven über endlichen Körpern.

Durch Iteration der Punktaddition wird eine Multiplikation von Kurvenpunkten mit ganzen Zahlen k definiert:

k*P=P+P+...+P (k-fache Summe).

Diese Multiplikation von Kurvenpunkten mit ganzen Zahlen kann leicht und schnell ausgeführt werden, wohingegen die Umkehraufgabe, die Berechnung sogenannter diskreter Logarithmen, normalerweise nur mit außergewöhnlichem Rechenaufwand gelöst werden kann. Hierfür gibt es keinen Algorithmus mit subexponentieller Laufzeit. Diese Punktmultiplikation stellt somit eine Einwegfunktion dar, weshalb sie bei Verfahren mit öffentlichen Schlüsseln, den sogenannten Public-Key-Verfahren, verwendet wird.

Nachfolgend wird anhand eines in Fig. 5 gezeigten Ausführungsbeispieles das erfindungsgemäße Verfahren zum Erzeugen von Pseudozufallszahlen erläutert.

Eine erste elliptische Kurve E über dem Körper GF(p) ist durch die folgende Gleichung gegeben:

$(y^2) \bmod p = (x^3 + 6x +$
$6050679034418465473882149660454552069529384067 71) \bmod p,$
wobei $p = 2^{160}-47=$
1461501637330902918203684832716283019655932542929.
p ist eine Primzahl mit 160 Bits.

Die elliptische Kurve E über GF(p) besitzt als Gruppenordnung
$\#E(GF(p)) = 7*q$ mit
q=208785948190128988314812461240940947434505754881.
q ist wiederum eine Primzahl mit 128 Bits.

Die Gruppenordnung einer elliptischen Kurve ist die Anzahl der Elemente der Punktgruppe, also die Anzahl der Lösungen der definierenden Gleichung der elliptischen Kurve E über GF(p). Je größer der maximale Primteiler der Gruppenordnung ist, desto schwieriger ist die Berechnung diskreter Logarithmen. Die Größe der Gruppenordnungen und ihrer maximalen Primteiler stellt somit ein Qualitätsmerkmal des erfindungsgemäßen Verfahrens dar, wobei die Gruppenordnungen vorzugsweise zumindest 2^{100} oder besser 2^{130} betragen sollten.

Eine zweite elliptische Kurve E' über GF(p) ist durch folgende Gleichung gegeben:

$(y^2) \bmod p = (x^3 + 3x + 168756385740498547400152923318200148712149363991) \bmod p.$

Die Kurve E' ist isogen zur Kurve E, das heißt, wenn die Kurve E die Form

$$y^2=x^3+ax+b$$

aufweist, besitzt die Kurve E' die Form

$$y^2=x^3+ac^2x+bc^3,$$

mit a, b, c aus GF(p), wobei c ein quadratischer Nichtrest modulo p ist. Im vorliegenden Fall gilt für c:

$c= 503145425704462245322517599589013227703324936803.$

Die Verwendung zweier isogener Kurven statt zweier beliebiger Kurven bietet wesentliche Vorteile. So kann man die Ordnung der elliptischen Kurve E' über GF(p) einfach aus der Gruppenordnung von E ableiten, da nämlich die Summe der beiden Ordnungen 2p+2 ist, womit sich folgende Gleichung ergibt:

WAVELYNX EX. 1003, Pg. 1787
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

#E'(GF(p)) = 2p+2 - #E(GF(p))

Im vorliegenden Fall ergibt sich für die Gruppenordnung von E':

#E'(GF(p)) = 2p+2 - #E(GF(p)) = 11 * 19 * q'
mit
q'= 458150983489311259624978820296545268736778934 7.

q' ist eine Primzahl mit einer Länge von 152 Bits.

Man wählt nun zwei Punkte P, P' der Kurven E, E', wie z.B.:

P =(27,1199480719563308855489368355308026541006624847440)
P' =(318,767790262932904318810390534329377261151321453045),
und
zwei Startwerte s, s', z.B. s=s'=2.

Durch die Bestimmung der elliptischen Kurven E, E', der Punkte P, P' und der Startwerte s, s' ist der Schritt S1 aus Fig. 5 abgeschlossen. Der Verfahrensablauf geht nun auf den Schritt S2 über, bei dem die Punkte P, P' mit s bzw. s' multipliziert werden, wobei das Ergebnis als PA bzw. PA' bezeichnet wird. Die Multiplikation wird als s-fache bzw. s´-fache Addition gemäß der in Fig. 3 gezeigten Addition ausgeführt.

Die Punkte PA und PA' werden der Vorschrift zum Ermitteln von Zufallsbits übergeben (Schritt S3). Im vorliegenden Fall werden die x-Koordinaten der beiden Punkte PA und PA' mit XOR verknüpft und durch c geteilt.

Für isogene elliptische Kurven E und E´ gilt, daß für ein beliebiges x aus GF(p) x entweder x-Koordinate von zwei verschiedenen Punkten auf E ist, oder aber x ist x-Koordinate eines Punktes auf E und cx ist x-Koordinate eines Punktes auf E', oder aber x ist nicht x-Koordinate eines Punktes auf E,

WAVELYNX EX. 1003, Pg. 1788
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

aber cx ist x-Koordinate von zwei Punkten auf E'. Wenn man also die x-Koordinaten auf E' durch c teilt, dann kommt jedes beliebige x aus GF(p) genau 2x als x-Koordinate vor. Das heißt, wenn man eine x-Koordinate auf E mit einer x-Koordinate auf E' geteilt durch c verknüpft, ist das äquivalent zum Verknüpfen zweier beliebiger, zufälliger Werte zwischen 0 und p-1. Die hierdurch abgeleiteten Pseudozufallsbits verhalten sich also wie echte Zufallsbits.

Vom Schritt S2 werden die Punkte PA und PA' auch an den Schritt S4 übergeben, bei dem die Punkte P, P' unverändert bleiben und s bzw. s' jeweils um eins erhöht wird.

Vom Schritt S4 geht der Verfahrensablauf wieder auf den Schritt S2 über, bei dem wiederum neue Punkte PA und PA' gebildet werden, die dann wieder an den Schritt S3 zur Berechnung weiterer Zufallsbits und an den Schritt S4 übergeben werden. Dieser Verfahrensablauf kann vielfach wiederholt werden, wobei immer wieder neue Zufallsbits erzeugt werden.

Die Erfinder der vorliegenden Erfindung haben mit dem oben beschriebenen Verfahren zum Erzeugen von Zufallszahlen 20 x eine Million Zufallsbits erzeugt und diese Zufallsbits verschiedenen statistischen Tests unterzogen. Mit den Tests konnten keine Abweichungen von echten Zufallsbits festgestellt werden.

Für die Erfindung ist wesentlich, daß im Schritt S3 die Zufallszahl Z aus den beiden Punkten PA und PA' ermittelt wird, die von unterschiedlichen elliptischen Kurven E und E' stammen. Durch das Verknüpfen dieser beiden Punkte PA und PA' wird sichergestellt, daß anhand der erzeugten Pseudozufallszahlen nicht die der Berechnung der Punkte PA und PA' zugrunde liegenden Punkte P und P´ durch diskrete Logarithmen ermittelt werden können. Von dem Ergebnis aus S3 kann somit nicht auf das Verfahren zum Erzeugen der Punkte PA, PA' mit

den Schritten S1, S2 und S4 geschlossen werden, was durch die gestrichelte Linie in Fig. 5 dargestellt ist.

Die Erfindung ist nicht auf das in Fig. 5 dargestellte Ausführungsbeispiel beschränkt. Im Rahmen der Erfindung ist es z.B. möglich, im Schritt S3 eine andere Verknüpfung der x-Koordinaten zu wählen. So können z.B. die beiden x-Koordinaten durch eine Addition modulo p miteinander verknüpft werden. Oder aber man verknüpft die y-Koordinaten. Oder aber x- und y-Koordinaten. Im Rahmen der Erfindung ist es auch möglich, daß anstelle von fest vorgegebenen elliptischen Kurven E, E' mit Punkten P, P' nach jeder Berechnung von PA und PA' neue Kurven E*, E*' und Punkte P*, P*' bestimmt werden, die zur Berechnung der nächsten Punkte PA* und PA*' herangezogen werden. Auch die Werte s, s' können an sich beliebig verändert werden. Für die Erfindung ist lediglich wesentlich, daß die Werte s, s' ganze Zahlen sind. Zu Beginn des Verfahrens können sie beispielsweise mit einem einfachen Zufallsgenerator erzeugt werden, der keinen hohen Ansprüchen genügen muß. In Fig. 6 ist das grundsätzliche Prinzip der vorliegenden Erfindung dargestellt, das eine Schleife bestehend aus den Schritten S5 und S6 aufweist, wobei in Schritt S5 zwei elliptische Kurven E, E', zwei Punkte P, P' auf den beiden Kurven und zwei Startwerte s, s' gewählt werden. Im Schritt S6 werden die Punkte P, P' mit s bzw. s' multipliziert, woraus sich PA und PA' ergibt. Bei jeder Wiederholung der Schleife S5, S6 wird zumindest eines der Paare E, E' bzw. P, P' bzw. s, s' verändert. Es ist auch möglich, zwei oder alle 3 Paare nach einer festzulegenden Regel zu verändern.

Bei jeder Wiederholung der Schleife wird ein neues Zahlenpaar PA, PA' erzeugt und dem Verfahrensschritt S7 übergeben, bei dem die beiden Punkte PA und PA' jeweils zu einer Pseudozufallszahl Z verknüpft werden.

Verfahren auf Basis elliptischer Kurven verwenden als Einwegfunktion die Multiplikation auf elliptischen Kurven, weshalb

Vorrichtungen zum Durchführen solcher Verfahren mit Routinen und Einrichtungen für Arithmetik auf elliptischen Kurven versehen sind. Solche Verfahren benötigen zudem Zufallszahlen zum Erstellen der privaten und öffentlichen Schlüssel. Durch Verwenden des erfindungsgemäßen Verfahrens zum Erzeugen dieser Zufallszahlen können zum einen qualitativ hochwertige Pseudozufallszahlen erzeugt, und zum anderen kann der Programmcode gering gehalten werden, da die vorhandenen Routinen doppelt verwendet werden können. Hierdurch werden erhebliche Ressourcen eingespart, und gleichzeitig wird die Sicherheit des Verfahrens deutlich gesteigert.

Fig. 7 zeigt schematisch den Aufbau eines Programmes zum Ausführen des erfindungsgemäßen Verfahrens in einem Blockschaltbild. Das Programm besteht aus einem Teil P1 zum Durchführen des Signaturverfahrens, das auf einen Programmteil P2 zurückgreift, mit dem Multiplikationen auf elliptischen Kurven über endlichen Körpern durchgeführt werden. Der Programmteil P1 wird von einem weiteren Programmteil P3 mit Zufallszahlen versorgt, wobei der Programmteil P3 wiederum auf den Programmteil P2 zum Multiplizieren auf elliptischen Kurven zurückgreift. Am Programmteil P1 ist ein Dateneingangsstrom I und ein Datenausgangsstrom O dargestellt, wobei der Dateneingangsstrom eine zu signierende Nachricht sein kann und der Datenausgangsstrom die Signatur. Ferner kann der Programmteil P1 am Datenausgangsstrom O seinen privaten und öffentlichen Schlüssel ausgeben. Diese Funktionen des Programmteils P1 entsprechen den an sich bekannten Signaturverfahren und -vorrichtungen auf Basis elliptischer Kurven. Das erfindungsgemäße Verfahren kann insbesondere bei Recheneinrichtungen mit geringerer Rechenkapazität, wie z.B. Chipkarten eingesetzt werden, da der entsprechende Programmcode äußerst kompakt ist und die Länge der zu verarbeitenden Zahlen wesentlich kürzer als bei einem RSA-Verfahren gleicher Sicherheitsstufe. Es ist jedoch auch möglich, die Programme auf elektronisch lesbaren Datenträgern zu vertreiben.

WAVELYNX EX. 1003, Pg. 1791
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Patentansprüche

1. Verfahren zum Erzeugen von Pseudozufallszahlen, bei dem zumindest zwei Punkte (P, P´) von zumindest zwei unterschiedlichen elliptischen Kurven (E, E´) über einem endlichen Körper (GF) bestimmt werden und eine Pseudozufallszahl durch Verknüpfen dieser Punkte (P, P´) erzeugt wird.

2. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 1, d a d u r c h g e k e n n z e i c h n e t, daß zur Bestimmung der Pseudozufallszahl jeweils ein Paar von Punkten (P, P´) bestimmt wird, wobei zur Bestimmung der einzelnen Paare jeweils dieselben zwei elliptischen Kurven (E, E´) verwendet werden.

3. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 2, d a d u r c h g e k e n n z e i c h n e t, daß die beiden elliptischen Kurven (E, E´) zueinander isogen sind.

4. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 3,
d a d u r c h g e k e n n z e i c h n e t, daß die Punkte (P, P´) eines ersten Paares in Abhängigkeit zweier Startwerte (s, s´) bestimmt werden.

5. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 4,
d a d u r c h g e k e n n z e i c h n e t, daß die Punkte (P, P´) der weiteren Paare durch Variieren der Startwerte gemäß einer vorbestimmten Regel bestimmt werden.

6. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 4,
d a d u r c h g e k e n n z e i c h n e t, daß die weiteren Paare von Punkten (P, P´) durch Variieren der elliptischen

Kurven und/oder der Punkte (P, P´) nach einer vorbestimmten Regel bestimmt werden.

7. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 6,
d a d u r c h g e k e n n z e i c h n e t, daß zum Ermitteln einer Zufallszahl die Koordinaten der beiden Punkte (P, P´) miteinander verknüpft werden.

8. Verfahren zum Erzeugen von Pseudozufallszahlen nach Anspruch 7,
d a d u r c h g e k e n n z e i c h n e t, daß die x-Koordinaten der beiden Punkte (P, P´) miteinander verknüpft werden, wobei die beiden elliptischen Kurven (E, E´) isogen sind.

9. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 8,
d a d u r c h g e k e n n z e i c h n e t, daß die Punktgruppen (E(GF (p)), E´(GF (p))) der elliptischen Kurven (E, E´) über einem endlichen Körper GF(p) Gruppenordnungen (q bzw. q´) von zumindest 2^{100} und vorzugsweise mindestens 2^{130} aufweisen.

10. Verfahren zum Erzeugen von Pseudozufallszahlen nach einem der Ansprüche 1 bis 9,
d a d u r c h g e k e n n z e i c h n e t, daß die elliptischen Kurven über dem endlichen Körper GF(p) definiert sind, wobei p eine Primzahl ist, die größer als 3 ist.

11. Verfahren für elektronische Signatur auf Basis elliptischer Kurven, bei dem die Schlüssel auf Grundlage von Zufallszahlen erzeugt werden,
d a d u r c h g e k e n n z e i c h n e t, daß die Zufallszahlen nach einem Verfahren der Ansprüche 1 bis 10 ermittelt werden.

WAVELYNX EX. 1003, Pg. 1793
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

12. Vorrichtung zur Durchführung des Verfahrens für elektronische Signatur auf Basis elliptischer Kurven nach Anspruch 11, mit

einer Einrichtung zum Ausführen von Multiplikationen in der Punktgruppe einer elliptischen Kurve (E, E´) über einem endlichen Körper (GF(p)),

einer Einrichtung zum Signieren, die die Einrichtung zum Ausführen der Multiplikation verwendet, und

einer Einrichtung zum Erzeugen von Pseudozufallszahlen nach dem Verfahren nach einem der Ansprüche 1 bis 9, wobei auch diese Einrichtung die Einrichtung zum Ausführen der Multiplikation verwendet.

WAVELYNX EX. 1003, Pg. 1794
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

FIG 1

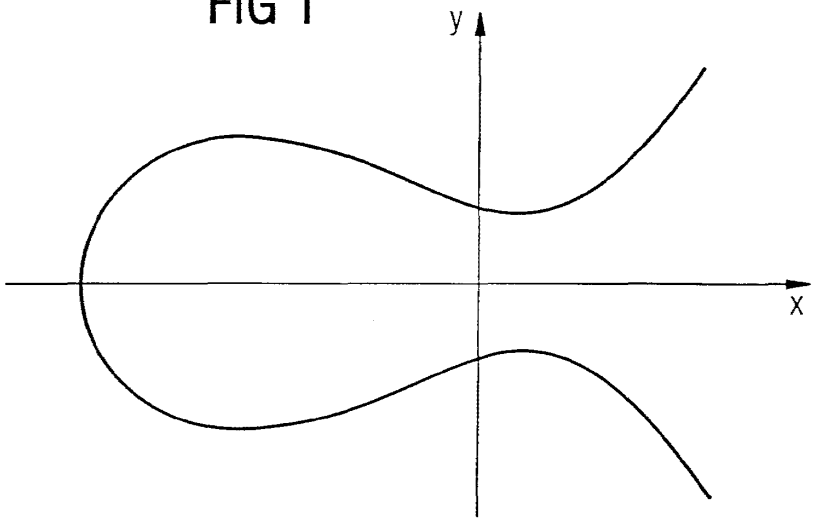


FIG 2

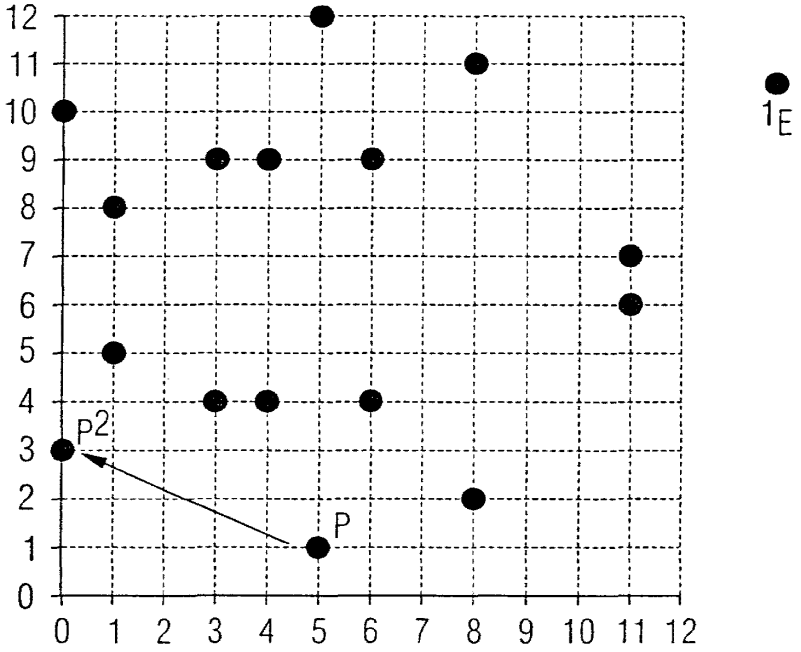


FIG 3

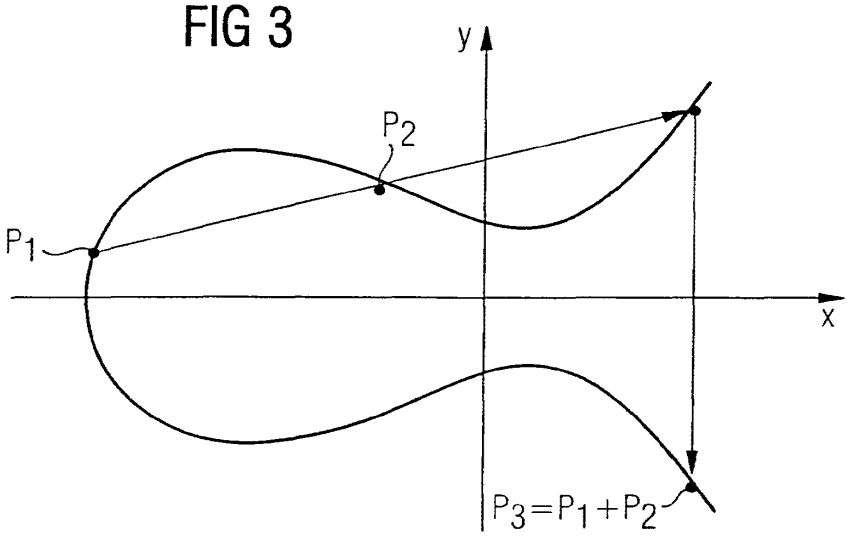


FIG 4

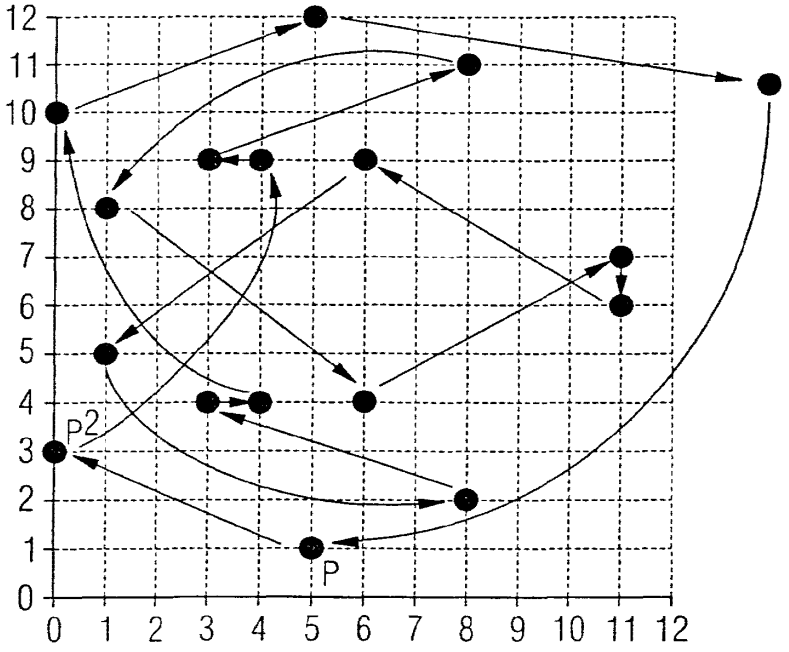


FIG 5

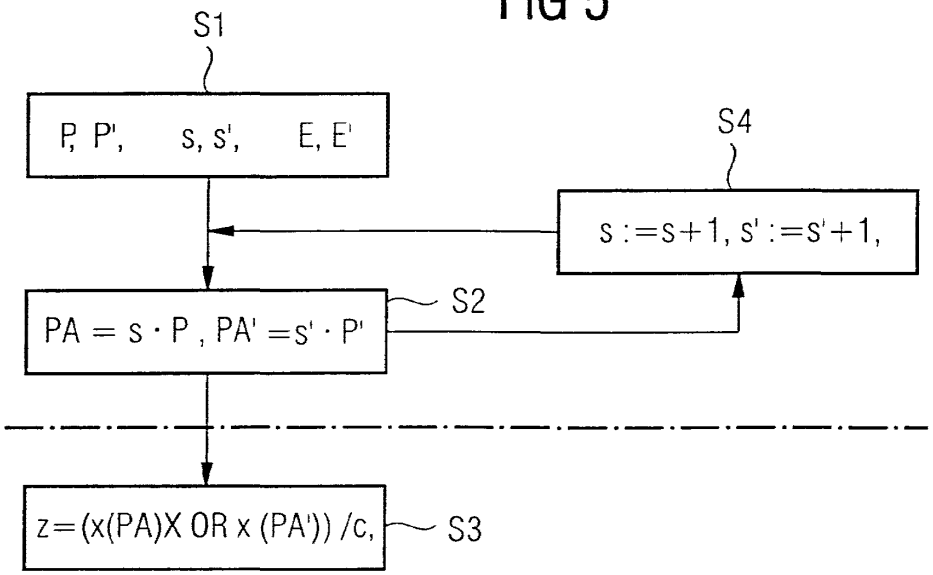

S1
P, P', s, s', E, E'
S4
s :=s+1, s' :=s'+1,
PA = s · P , PA' =s' · P'
S2
z=(x(PA)X OR x (PA')) /c,
S3

FIG 6

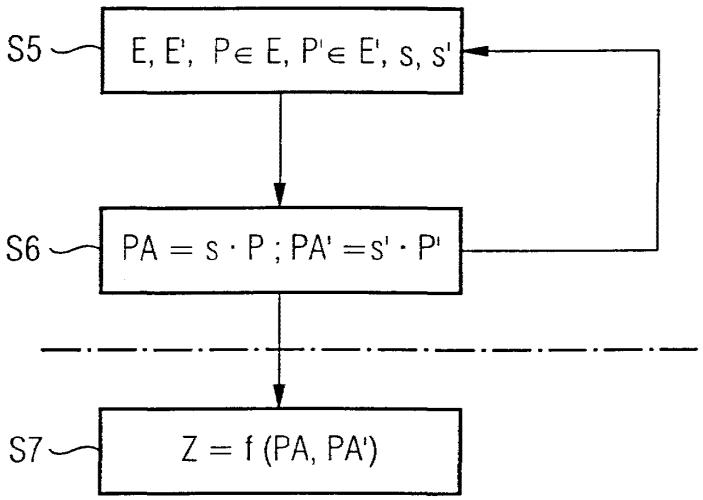
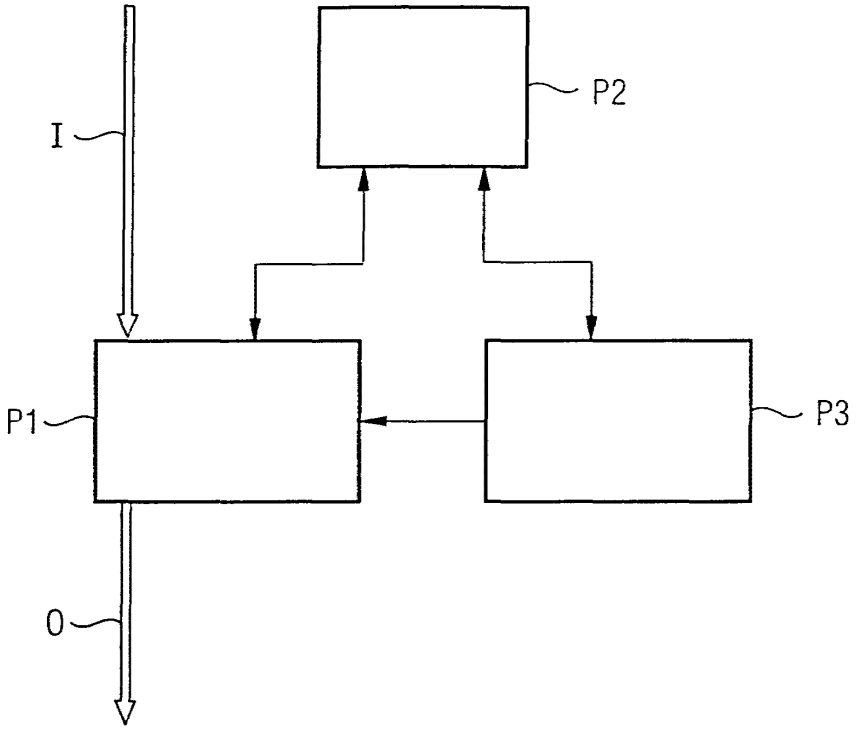

S5
E, E', P∈ E, P'∈ E', s, s'
S6
PA = s · P ; PA' =s' · P'
S7
Z = f (PA, PA')

FIG 7



WAVELYNX EX. 1003, Pg. 1798
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/DE 00/02776

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/58 H04L9/32 //G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H03K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KALISKI B S JR: "One-way permutations on elliptic curves" JOURNAL OF CRYPTOLOGY, 1991, USA, vol. 3, no. 3, pages 187-199, XP000972491 ISSN: 0933-2790 page 187, paragraph 1 page 188, paragraph 7 page 194, paragraph 2 -page 196, paragraph 1 ---	1-12
X	KALISKI B S: "A PSEUDO-RANDOM BIT GENERATOR BASED ON ELLIPTIC LOGARITHMS" PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES (CRYPTO),DE,BERLIN, SPRINGER, vol. CONF. 6, 1986, pages 84-103, XP000090665 page 98, line 20 - line 33 -----	1-12

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 December 2000	20/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Verhoof, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

WAVELYNX EX. 1003, Pg. 1799
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/DE 00/02776

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F7/58 H04L9/32 //G06F7/72

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F H03K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	KALISKI B S JR: "One-way permutations on elliptic curves" JOURNAL OF CRYPTOLOGY, 1991, USA, Bd. 3, Nr. 3, Seiten 187-199, XP000972491 ISSN: 0933-2790 Seite 187, Absatz 1 Seite 188, Absatz 7 Seite 194, Absatz 2 -Seite 196, Absatz 1 ---	1-12
X	KALISKI B S: "A PSEUDO-RANDOM BIT GENERATOR BASED ON ELLIPTIC LOGARITHMS" PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES (CRYPTO),DE,BERLIN, SPRINGER, Bd. CONF. 6, 1986, Seiten 84-103, XP000090665 Seite 98, Zeile 20 - Zeile 33 -----	1-12

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☐ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
8. Dezember 2000	20/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Verhoof, P

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/010373 A1

(51) International Patent Classification[7]: G06K 019/07

(21) International Application Number:
PCT/AU2003/000934

(22) International Filing Date: 23 July 2003 (23.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/AU02/00984 24 July 2002 (24.07.2002) AU

(71) Applicant *(for all designated States except US)*: **BANQUE-TEC INTERNATIONAL PTY LTD** [AU/AU]; Unit 5, 12-18 Victoria Street, East Lidcombe, NSW 2141 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **BLAKE, Christopher, Ian** [AU/AU]; C/o Banque-Tec International, Unite 5, 12-18 Victoria Street, East Lidcombe, NSW 2141 (AU).

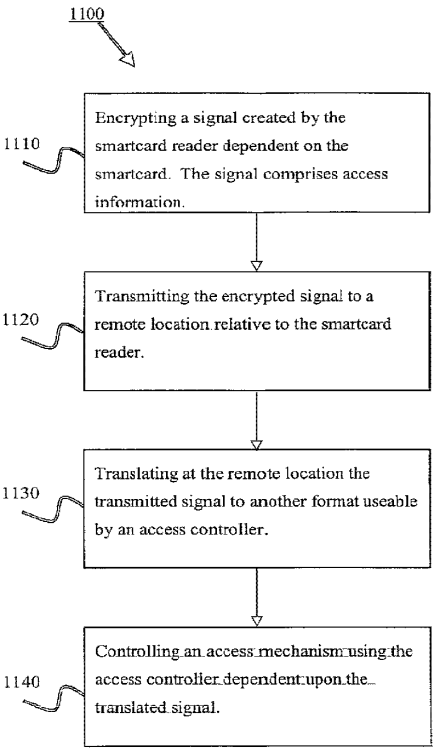
(74) Agent: **SPRUSON & FERGUSON**; G.P. Box 3898, Sydney, NSW 2001 (AU).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: A METHOD OF SECURE TRANSMISSION



(57) Abstract: A method, a system, and an apparatus for providing secure transmissions from a smartcard reader are described. A signal created by the smartcard reader dependent on the smartcard is encrypted. The signal comprises access information. The encrypted signal is transmitted to a remote location relative to the smartcard reader. The transmitted signal is translated at the remote location to another format useable by an access controller. An access mechanism is controlled using the access controller dependent upon the translated signal.

WO 2004/010373 A1

WAVELYNX EX. 1003, Pg. 1801
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A METHOD OF SECURE TRANSMISSION

Field of the Invention

The present invention relates generally to security systems and in particular to secure transmission systems and security systems utilising biometric sensors.

Background

Existing security systems are of several different types. One type of security system utilises a smartcard as a key for access to a secure location or secure equipment. The smartcard contains security information providing access via a smartcard reader at the access point. A user presents the reader with the smartcard. If the smartcard is authorised, the reader actuates a control mechanism to provide access. Thus, for example, the reader may signal a controller that controls operation of a latch mechanism controlling access to a door or provide access to a computer terminal. One example of a relevant reader that may be used in such a system is a Wiegand reader. One significant disadvantage of such systems is that the smartcard if stolen or otherwise in the possession of an unauthorised person may allow the unauthorised person to access the secure location or equipment.

Another security system utilises a biometric sensor to control access. A user must provide biometric data, normally a fingerprint, speech, or an eye scan via a sensor at the access point. Other forms of biometric data include facial details and hand geometry. Biometrics is a physical characteristic of a person used as a form of identification. The biometrics data is used in place of, or in addition to a security key, such as a key, card or PIN. A database or central repository of stored biometric data is maintained in a computer, with which the sensor can communicate. The scanned biometric data is compared with the stored biometric data, and if a match is found the user is permitted access. This system is generally more secure than that of the smartcard system, but is disadvantageous in that a central repository of biometric data must be maintained and updated. Further, significant time may be required to conduct such a comparison of the scanned biometric data against the database or central repository to determine whether or not there is a match.

Conventional systems are also disadvantageous in that the products' sizes are bulky. Still a further disadvantage of conventional systems is that such products cannot protect against security breaches arising from a person getting into security lines in a wall to which the reader is connected and providing false authorisation signals and the like to a controller.

Summary

In accordance with an aspect of the invention, there is provided a method of providing secure transmissions from a smartcard reader. The method comprises the steps of: encrypting a signal created by the smartcard reader dependent on the smartcard, the signal comprising access information; transmitting the encrypted signal to a remote location relative to the smartcard reader; translating at the remote location the transmitted signal to another format useable by an access controller; and controlling an access mechanism using the access controller dependent upon the translated signal.

The smartcard may contain biometric data and the smartcard reader may comprise a biometric smartcard reader for obtaining biometric data directly. The biometric data may comprise fingerprint data. The biometric data is not transmitted to the remote location from the smartcard reader.

The method may further comprise the step of providing access using the access mechanism if the translated signal is determined by the access controller to authorise access. The access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation. The access information may comprise at least one of a person's name, a facility code, a company code, an access code, and an issue code. The signal may be encrypted using triple DES, Skipjack, or AES Rijndael encryption.

The method may further comprise the step of encrypting communications between the smartcard and the smartcard reader. The encrypted signal may be

transmitted from the smartcard reader to a high security module at the remote location. The high security module translates the encrypted signal to the other format.

The smartcard reader and the high security module may be separated by a distance of up to 1.2 kilometres. Alternatively, the smartcard reader and the high security module are separated by a distance of up to 15 metres.

The translated signal may be in a controller-specified format. Preferably, the controller-specified format is Wiegand format, or clock and data.

In accordance with another aspect of the invention, there is provided a system for providing secure transmissions from a smartcard reader. The system comprises: a smartcard reader for encrypting a signal created by the smartcard reader dependent on the smartcard, the signal comprising access information, and for transmitting the encrypted signal to a remote location relative to the smartcard reader; a high security module for receiving the transmitted signal and translating the transmitted signal to another format useable by an access controller; and an access controller for controlling an access mechanism using the access controller dependent upon the translated signal.

The smartcard may contain biometric data, and the smartcard reader may comprise a biometric smartcard reader for obtaining biometric data directly. The biometric data may comprise fingerprint data. The biometric data is not transmitted to the high security module from the smartcard reader.

The system may further comprise an access mechanism providing access if the translated signal is determined by the access controller to authorise access. The access mechanism may be able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation. The access information may comprise at least one of a person's name, a facility code, a company code, an access code, and an issue code.

The signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption. Communications between the smartcard and the smartcard reader may be encrypted. The smartcard reader and the high security module may be separated by a distance of up to 1.2 kilometres. Alternatively, the smartcard reader and the high security module may be separated by a distance of up to 15 metres.

The translated signal may be in a controller-specified format. The controller-specified format may be Wiegand format, or clock and data.

In accordance with still another aspect of the invention, there is provided an apparatus for providing secure transmissions from a smartcard reader. The apparatus comprises: a smartcard reader for encrypting a signal created by the smartcard reader dependent on the smartcard, the signal comprising access information; a module for transmitting the encrypted signal to a remote location relative to the smartcard reader; a module for translating at the remote location the transmitted signal to another format useable by an access controller; and an access controller for controlling an access mechanism dependent upon the translated signal.

The smartcard may contain biometric data and the smartcard reader may comprise a biometric smartcard reader for obtaining biometric data directly. The biometric data may comprise fingerprint data.

In accordance with a further aspect of the invention, identification using of biometric data is disclosed. A smartcard encoded with biometric data is read. Actual biometric data is sensed. The biometric data from the smartcard is then compared with the sensed biometric data for verification. Access may be allowed if the biometric data from the smartcard and the sensed biometric data match. This may involve verifying that the biometric data encoded on the smartcard is correct. The biometric data stored in the smartcard is derived by scanning a source of biometric data associated with the smartcard, encoding the scanned biometric data, and storing the encoded biometric data on the smartcard. The biometric data may include a fingerprint. Optionally, a detail level can be specified for scanning the biometric data.

Brief Description of the Drawings

A small number of embodiments are described hereinafter with reference to the drawings, in which:

Fig. 1 is a high-level flow diagram illustrating an enrolment operation of a biometric smartcard system including a biometric smartcard reader or encoder in accordance with an embodiment of the invention;

Fig. 2 is a flow diagram illustrating a process of enrolling a fingerprint on a smartcard using a biometric smartcard encoder, providing further details of the embodiment of Fig. 1;

Fig. 3 is a flow diagram illustrating a process of verifying a finger on the biometric smartcard encoder, providing further details of the embodiment of Fig. 1;

Fig. 4A is a block diagram illustrating the structure of storage or memory in a smartcard in accordance with the embodiment of the invention;

Fig. 4B is a table illustrating an arrangement of security keys used in the smartcard of Fig. 4A in accordance with the embodiment of the invention;

Fig. 5 is a functional block diagram showing modules of a biometric smartcard reader or encoder in accordance with the embodiment of the invention;

Fig. 6 is a perspective view of a biometric smartcard reader or encoder in accordance with the embodiment of the invention shown in Fig. 5;

Fig. 7 is a block diagram of a secure transmission system in accordance with a further embodiment of the invention;

Fig. 8 is a flow diagram illustrating a process of secure transmission in accordance with the further embodiment of the invention, which may be practiced with the system of Fig. 7;

Fig. 9 is a block diagram of a secure transmission system in accordance with another embodiment of the invention;

Fig. 10 is a block diagram of a secure transmission system in accordance with still another embodiment of the invention; and

Fig. 11 is a flow diagram illustrating a process of providing secure transmissions from a smartcard reader in accordance with a further embodiment of the invention.

Detailed Description

A method, an apparatus, and a system for biometric smartcard reading and encoding, as well as for secure transmissions are described hereinafter. Numerous specific details are set forth. However, it will be apparent to those skilled in the art in the light of this disclosure that various modifications may be made without departing from the scope and spirit of the invention. Embodiments of the invention provide equipment that synthesise biometric and smartcard technologies to provide a smartcard reader or encoder that eliminates central database communications infrastructure. As the smartcard holds the biometric information, the requirement of central repositories of biometric data and associated security issues are obviated. A significant application of the reader or encoder is as an access control device at security point, whether for access via a door or other portal, or to a computer, network, or other secure equipment or installation.

In the following description, the terms biometric smartcard reader and biometric smartcard encoder are used. A reader is a device that is able to scan a person's biometric data and contactlessly read a smartcard to obtain stored biometric data. The biometric data is preferably a fingerprint. The smartcard is presented to the reader (preferably, 10 mm to 40 mm away), and write/read operations are communicated from the reader to the smartcard. The reader then compares the scanned biometric data and stored biometric data to determine if there is a match. The reader may be located at an access point to provide access to a location or equipment in a security system dependent on the results of the comparison. An encoder is able to perform the functions of a reader including contactless communications with the smartcard, but also is able to encode a smartcard with personal details and biometric data. More particularly, the encoder preferably includes a logical access system where all access in a facility is controlled using a card, i.e. for doors, for PC access, etc. Such a smartcard access system by its nature almost ensures that the user does not forget to leave the smartcard behind. Preferably, an encoder has an appropriate interface to enable the encoder to be connected with a computer to enrol a person's details and biometric data on the smartcard using software running on the computer. The encoder stores biometric data in a two-dimensional structure or template and card holder details on the smartcard. The encoder may have an insert slot in the housing body to receive such a smartcard. The slot allows detection of

the smartcard during an encoding process. A reader cannot be used for enrolment of biometric data and other associated information on a smartcard as can an encoder. For ease of description, the following text uses the two terms biometric smartcard reader and biometric smartcard encoder substantially interchangeably, but the noted distinctions should be borne in mind.

Biometric Smartcard Reader or Encoder

In accordance with an embodiment of the invention, a biometric smartcard reader or encoder is disclosed. Fig. 5 is a block diagram illustrating a smartcard 540 and a biometric smartcard reader 500 in accordance with an embodiment of the invention. This biometric smartcard reader 500 is smaller than other biometric units. The biometric smartcard reader 500 includes a biometric sensor 510 coupled to a sensor control module or printed circuit board 520. The sensor PCB 520 contains modules for processing and encoding scanned biometric data into a suitable digital representation using a given coding algorithm (e.g., Sagem). The fingerprint is stored as a template preferably and not as a digital image. An algorithm is used to generate the template. For fingerprints, examples of relevant algorithms use minutiae reference points, or ridge recognition patterns, for example. In turn, the sensor PCB 520 is coupled to a smartcard reader PCB 530 and sends fingerprint data in a given template to the smartcard reader PCB 530, which is also able to interrogate and obtain data from a smartcard 540. This is preferably done by presenting the smartcard reader PCB 530 with the smartcard 540, in which the smartcard reader PCB 530 energises the smartcard 540 if in close proximity and communicates with the smartcard 540. Preferably, the smartcard reader PCB 530 is a contactless reader using a Philips Chip Mifare® utilising the Wiegand format for its output. Communication between the smartcard 540 and the smartcard reader PCB 530 is encrypted. The encryption utilised with this embodiment involves a proprietary encryption method of Mifare®, which is embedded in the Mifare® smartcards. Another option is to use DES encryption. However, it will be apparent to those skilled in the art in the light of this disclosure that other encryption techniques may be used without departing from the scope and spirit of the invention.

More preferably, the biometric smartcard reader 500 incorporates a biometric finger scan sensor 510 (e.g., for scanning fingerprints) with an accompanying sensor PCB 520. The fingerprint sensor technology may be optical, capacitive, thermal, tactile, or a combination of the foregoing. An example of a sensor arrangement that may be used is a Bioscrypt product provided by Bioscrypt Inc. including an Authentic sensor, a Bioscrypt PCB, and Bioscrypt's own encoding algorithm. Alternatively, the sensor arrangement may be implemented using an ST sensor, a Yuean PCB provided by Yuean Biometrics, and the Sagem algorithm, or a SecuGen product provided by SecuGen Corporation including a SecuGen sensor, a SecuGen PCB, and the SecuGen algorithm. Still further, a SecuGen optical solution may be practiced that enables a rugged and robust design. However, it will be apparent to those skilled in the art in the light of this disclosure that other biometric sensors may be practiced without departing from the scope and spirit of the invention. The sensor 510 and associated PCB 520 scan a person's fingerprint and generate a digital representation of that fingerprint as digital biometric data. Fig. 6 is a perspective view of a biometric smartcard reader 600, which embodies the reader 500 of Fig. 5 including a biometric sensor 610/510, an associated sensor PCB 520 (not shown), and a Mifare® smartcard reader PCB 530 (not shown) in a single unit.

The smartcard 540 is adapted to store a digital representation of the biometric data. Preferably, the smartcard is a Mifare® smartcard for use with the contactless Mifare® reader. The smartcard 540 has approximately 1 Kbyte of storage or memory. Fig. 4A is a block diagram illustrating the structure of the storage 400 in the Mifare® smartcard, which is organised into 16 separate sectors 410-414 -- 0 sector 410, 1 sector 412, ..., 15 sector 414. Each of the sectors 410-414 has two keys, Key A and Key B as shown in Fig. 4B. These keys can be designated as read and read/write keys. The keys A and B for each sector are initialised by the manufacturer (e.g. 10 hexadecimal characters each) and can be changed when the sectors are written to to contain biometric data in accordance with the embodiment of the invention. Each Mifare® smartcard 540 also has a unique serial number or identifier. Preferably, the 15th sector 414 contains one or more of the following security parameters for use in the system of Fig. 5: a facility code, a company code, an access code, and an issue code. The facility code can identify a facility that the smartcard permits access to for a given entity or company, which is identified by

the company code. The issue code identifies how many smartcards have been issued to a person. For example, if the issue code is 3, the system may hotlist corresponding smartcards for the person with issue codes of 1 or 2.

Dependent upon the format of the digital biometric data, the smartcard 540 stores such data across two or more sectors with corresponding keys for each sector of data. In the preferred embodiment, 5 to 6 sectors are used to store a digital fingerprint representation or template. For example, an ST sensor and an Yuean PCB produce a digital fingerprint representation that is approximately 320 bytes long. The length of the representation may vary depending on the different biometric sensor products and algorithms used. As noted above, each sector needs a customer specific key to unlock the information.

Optionally, the reader 500/600 incorporates a tamper switch so that if a reader is pulled from a wall, the reader does not function and an alarm flag is activated.

As described in greater detail below, use of the biometrics smartcard encoder 500 enables authorised persons using a properly enrolled smartcard to access to a secure location or equipment, for example. Lost or stolen smartcards 540 are unusable as the person with the lost or stolen smartcard 540 does not have the correct biometrics data (e.g., fingerprint) to match that stored on the smartcard 540. Still further, another advantage of this embodiment is that the biometric smartcard reader 500 of Fig. 5 obviates the need for a central database or repository of biometric data, since the biometrics data is stored on the smartcard 540.

In combination with a computer (not shown), a biometrics smartcard encoder 500 can also be used to enrol a person's fingerprint on a smartcard 540. The biometrics smartcard encoder 500 uses an RS232 or USB communications port, in conjunction with software, to enrol the person's fingerprint onto the smartcard 540. Generally, software or a computer program(s) running on the computer in combination with the biometrics smartcard encoder 500 obtains personal details for a person, scans and records a fingerprint for the person, and then writes the personal details and fingerprint

representation to the smartcard 540. Preferably, this embodiment does not permit fingerprint information to travel to the computer. Instead, the biometric smartcard encoder 500 stores the information and writes the information directly to the smartcard 540. The information is then erased from the memory of the biometric smartcard encoder 500. When enrolling a person's fingerprint, the detail level for scanning by the biometric smartcard encoder 500 can be changed to enable persons with scarred hands or other aberrations to use the encoder 500. This process is set forth in greater detail with reference to Fig. 1.

Fig. 1 is a high-level flow diagram illustrating details of a process 100 of obtaining and storing biometric information in a smartcard 540 using the biometric smartcard encoder (i.e., biometric unit) 500/600. In state 110, the biometric smartcard encoder 500 is initially idle. In step 112, a command is sent to the biometric smartcard encoder 500 to capture a person's fingerprint. This is preferably done by the computer using a communications port. In step 114, the sensor 510/610 of the biometric smartcard encoder 500 captures a fingerprint image. The sensor 510/610 analyses the scanned fingerprint and creates an image. In step 116, the image is coded and the data to be stored is created. This is preferably done by the sensor PCB 520 in combination with the sensor 510. In step 118, the smartcard 540 is presented to the smartcard reader PCB 530, and the biometric data from the sensor PCB 520 is written into the smartcard 540 by the smartcard reader PCB 530. State 120 at the end of the process 100 shows that the digital fingerprint representation is stored on the smartcard 540. This smartcard 540 can then be used as a security key in relation to a biometric security system.

Generally, when verification or access is required using a biometric smartcard reader 500/600, the smartcard 540 is presented to the biometric smartcard reader 500/600 and the fingerprint information is read off the smartcard 540 by the biometric smartcard reader 500/600. The person then presents their finger to the sensor 510/610 of the biometric smartcard reader 500/600 for scanning. The fingerprint representation read off the smartcard 540 is compared by the biometric smartcard reader 500/600 with the fingerprint currently obtained using the sensor 510/610. If there is a match within the detail level set at enrolment, the biometric smartcard reader 500/600 checks access

privileges using the access code from the smartcard 540 and if the holder has appropriate access privileges, access is granted by the biometric smartcard reader 500/600 to the smartcard holder. Verification is strongly dependent on enrolment. A score of 100 applies for a high quality and content template. A medium threshold level may look for a score of 60, for example. The threshold level may be varied to adjust quality and content of a template.

Details of Enrolment Process

Fig. 2 is a more detailed flow diagram of a process 200 of enrolling a fingerprint using a biometric smartcard encoder, based on Fig. 1. In an initial state 210, a biometric software application is run or launched. As noted above, this software is run on a computer connected to a biometric smartcard encoder 500/600, preferably using a RS232 or USB communications port. In step 212, a relevant RS232 or USB port (denoted generally by COM in Fig. 2) is selected by the software. Other interfaces may be practiced without departing from the scope and spirit of the invention. In step 214, the communications link (COM port) is tested to ensure the communications link is operating properly. Communication between the smartcard reader PCB 530 and the computer is preferably triple DES or Skipjack encrypted. Therefore, the information sent for access to the computer is highly difficult to compromise. In step 216, enrolment of a person's fingerprint is commenced. Preferably, this is done by clicking on an enrolment tab in the software application to commence enrolment processing. In step 218, personal details of the person whose fingerprint is to be enrolled are obtained and the type of smartcard being written to is specified. The relevant information may include one or more of the person's name, facility code, company code, access code, and issue code. Alternatively, the smartcard may be pre-encoded with some or all of this information.

In step 220, the desired detail level of the fingerprint is specified using the software application. In particular, this is done using a quality meter in the software where the detail level for the sensor 510 and PCB 520 is specified. Ordinarily, the quality is set as high as possible to avoid misreads. However, the quality can be adjusted downwardly to avoid or reduce the effects of scar tissue and other aberrations on the person's finger. In step 222, the person's fingerprint is presented to the sensor 510/610 of

the biometric smartcard encoder 500/600, and the person's fingerprint is scanned. The data stream for the scanned fingerprint is sent from the sensor 510/610 to the sensor PCB 520. The information is then coded with the specific algorithm within the sensor PCB 520. The coded information is then sent to the smartcard reader PCB 530 and from there encoded onto the smartcard 540.

In decision block 224, a check is made to determine if the quality of the scanned fingerprint image from the sensor 510/610 is adequate. The sensor 510 and PCB 520 determines quality. The biometric smartcard encoder 500/600 indicates this to the computer, since the fingerprint is preferably not transferred to the computer. If the quality is inadequate (NO), the quality is reduced to enable enrolment in step 226 and processing continues at step 222. This may occur multiple times. If decision block 224 determines that the quality is adequate (YES), processing continues at step 228.

In step 228, a smartcard 540 is presented to the smartcard reader PCB 530 of the biometric smartcard encoder 500/600. Presentation of the smartcard 540 to the smartcard reader PCB 530 results in the encoded fingerprint template and related keys for each sector being downloaded onto the smartcard 540. The communication between the smartcard 540 and the reader PCB 530 is encrypted. As noted above, the encrypted, encoded fingerprint representation is normally stored across several sectors in the storage of the smartcard. Also personal details and other information may be stored on the smartcard 540. In step 230, a check is made to determine if the encoding of the smartcard 540 was successful. If decision block 230 returns true (YES), the fingerprint template has been encoded successfully on the smartcard 540 using the encoder 500. If decision block 230 returns false (NO), processing continues at decision block 232. In decision block 232, a check is made to determine if the smartcard type details are correct. For example, the smartcard 540 may be a new or used smartcard. A new smartcard has default values in its storage, while a used smartcard has changed keys A and B for example. Further, or alternatively, a different type of smartcard may be used, for example, from different manufacturers. If decision block 232 returns false (NO) indicating the card type details are incorrect, processing continues at step 234 and the correct smartcard type must be specified to the software. Processing then continues at step 236. If decision block 232

returns true (YES), processing continues at step 236. In step 236, another smartcard is tried or obtained for presentation instead of the smartcard previously presented to the smartcard reader PCB 530 of the encoder 500/600. Processing then continues at step 228.

Details of Verification Process

After a fingerprint representation and associated information are enrolled on a smartcard 540, verification of the enrolment on the smartcard 540 may be required. Fig. 3 is a flow diagram illustrating a process 300 of verifying a fingerprint scanned by the biometric smartcard encoder 500/600 and enrolled on the smartcard 540. In state 310, the biometric application software is loaded. In step 312, the communications link (COM port or USB) between the computer and the biometric smartcard encoder 500 is selected. In step 314, the communications link is tested to ensure the link is operating properly. In step 316, a verification application module in the software is activated. Preferably, this is done by clicking on a verify tab in the biometric application software. In step 318, the smartcard 540 with enrolled fingerprint information is presented to the encoder 500/600, which reads and stores the fingerprint information from the smartcard 540. In step 320, the person's finger is presented to sensor 510/610 of the biometric smartcard encoder 500, and the person's fingerprint is scanned and stored. The biometric smartcard encoder 500 then compares in the smartcard reader PCB 530 the scanned fingerprint template from the sensor 510/610 and the uploaded fingerprint template from the smartcard 540.

In decision block 322, a check is made to determine if the verification passed (OK). The encoder 500/600 provides the comparison result to the computer to establish verification. If decision block 322 returns true (YES), processing continues at state 324 and the fingerprint on the smartcard is verified as that of the fingerprint obtained at the sensor 510/610. Otherwise, if decision block 322 returns false (NO), processing continues at step 326. In step 326, a check is made to determine if the verification bar in the software was raised. Preferably, a quality bar and a verification bar showing current levels are depicted graphically to an operator of the application software on opposite sides of a graphical image of a fingerprint icon, which indicates to the operator when a fingerprint has been properly scanned by the encoder 500/600. Raising the verification bar indicates a better match between the scanned fingerprint and the one from the

smartcard 540. Verification is dependent on the quality level at enrolment. If decision block 326 returns true (YES), processing continues at step 332 and the finger must be positioned correctly for verification, before processing continues at step 320. Otherwise, if decision block 326 returns false (NO), processing continues at step 328. A determination is made that the incorrect finger has been used in relation to the recorded fingerprint information on the smartcard. In step 330, the correct finger is determined before proceeding to step 320.

Secure Transmission System

In a security system, a smartcard reader may be setup to give access on a per door basis or to equipment. The smartcard has unique keys that must also be contained in a smartcard reader's firmware. The smartcard reader communicates with the smartcard and information is read from the smartcard for access. The smartcard reader ordinarily communicates with an access controller, and this controller controls access; for example the controller may preferably activate a door latch for access. Information is sent to the controller. Communication between the smartcard reader and the controller is usually Wiegand. However, the communications may be RS485 or RS232. Still further, another example of a common form of communication back to a controller is Clock and Data. These formats can be cracked or defeated given time, as formats are usually 'known' industry standards. The controller determines whether or not to grant access and activates an access mechanism if granted. When using a security access reader to grant or deny access, a possible breach in security lies in the information that is directly sent to the controller by the smartcard reader. If the smartcard reader is removed from a wall or other connection point and a signal is introduced to the line between the smartcard reader and the controller, then a security breach exists. The signal may provide information to the controller so that the controller improperly grants access. If the smartcard reader has a tamper switch, a degree of added security is provided. A hole in the wall may still be made conditional to the material of the wall, and a security breach may still occur, as this enables access to the cables of the reader. In contrast, a stand-alone reader does not need a controller so this does not apply to such a reader.

In accordance with a further embodiment of the invention, secure transmission from a smartcard reader is provided by encrypting the messages from the smartcard reader in the security system. Preferably, the smartcard reader is a biometrics smartcard reader 500/600, but ordinary smartcard readers may be practiced. The further embodiment of the invention shown in Figs. 7 and 8 addresses this issue. This applies to the embodiments of Figs. 9-11 as well.

Fig. 7 is a block diagram of a secure transmission system 700 in accordance with the further embodiment of the invention. A smartcard reader 702 is coupled to a high security module (HSM) 704. Preferably, the smartcard reader 702 is a biometrics smartcard reader 500/600, but may be a standard smartcard reader. The HSM 704 is located remotely from the smartcard reader 702 and preferably at an inaccessible location relative to the smartcard reader 702, for example on the other side of a wall in a secure area. The distance between the smartcard reader 702 and the HSM 704 may be up to 15 metres. Communications between the reader 702 and the HSM 704 are preferably Triple DES or Skipjack encrypted, but other encryption techniques may be employed. The HSM 704 is in turn coupled to a controller 706. Communications between the HSM 704 and the controller 706 are carried out using the controller-specified format, which is usually Wiegand format but may be another format (e.g., clock and data). In turn, the controller 706 is connected to the door latch 708 to control operation of the door for access. Different access mechanisms may be used in place of a door latch 708, for example to provide access to a computer.

Significantly, the system 700 uses an HSM 704 for each access point and encrypted communications between the smartcard reader 702 and the HSM 704. The smartcard reader 702 preferably reads the information off a smartcard and communicates with the HSM 704 on the secure side of the wall, up to 15 metres away. Again, the communication is encrypted, preferably using a 3DES or Skipjack encrypted protocol. The HSM 704 decrypts the message to obtain the security information from the smartcard, e.g. "Facility Code" and the "Access number", and communicates these values to the access controller 706. Thus, communication between the smartcard reader 702 and the HSM 704 and thus the controller 706 is secure whether the smartcard reader 702 is

removed from the wall or wiring is accessed through a wall. This provides a higher standard of security for access control systems.

Fig. 8 is a flow diagram illustrating a process 800 for secure transmission. In state 810, the smartcard reader 702 is in standby mode. In step 812, a smartcard is presented for access. In step 814, the smartcard reader 702 reads and analyses access information on the smartcard. The smartcard and the reader must have the same keys. If a standard smartcard reader is used, an encrypted transmission is sent to the HSM 704 in step 816. Processing then continues at step 824. Otherwise, if a biometric smartcard reader 500/600 is used, after step 814, processing continues at step 818. In step 818, biometric data is obtained from the cardholder using the biometric sensor of the biometric smartcard reader 500/600 as reader 702. Preferably, the biometric data is fingerprint information. In step 820, the biometric data of the cardholder and the stored biometric data from the smartcard are compared and confirmed to be the same person or not. If the biometric data matches, in step 822, an encrypted transmission for access is sent to the HSM 704 from smartcard reader 702, before processing continues at step 824. In step 824, the HSM 704 decrypts the transmission and communicates it to the controller 706 using the appropriate controller format, e.g. Wiegand. The controller 706 either grants access 828 in step 826 or denies access 832 in step 830 dependent upon the access rights obtained from the smartcard.

Further Embodiments of Secure Transmission System

Fig. 11 is a flow diagram illustrating a method 1100 of providing secure transmissions from a smartcard reader in accordance with an embodiment of the invention. In step 1110, a signal created by the smartcard reader dependent on the smartcard is encrypted. The signal comprises access information. In step 1120, the encrypted signal is transmitted to a remote location relative to the smartcard reader. In step 1130, the transmitted signal is translated at a remote location to another format useable by an access controller. In step 1140, an access mechanism is controlled using the access controller dependent upon the translated signal. The smartcard may contain biometric data and the smartcard reader may comprise a biometric smartcard reader for obtaining biometric data

directly. The biometric data may comprise fingerprint data. The biometric data is not transmitted to the remote location from the smartcard reader.

Figs. 9 and 10 are block diagrams of secure transmission systems in accordance with further embodiments of the invention. In these drawings, modules with similar functionality to those of the modules shown in Fig. 7 are indicated with corresponding reference numbers, except that the leading digit(s) is replaced to correspond with the Figure number (e.g., the access controller 906 of Fig. 9 corresponds to the access controller 706 of Fig. 7). For the sake of brevity only, aspects of the smartcard reader and security system are not repeated hereinafter, but reference is made to the description accompanying Figs. 7 and 8. Further, the door latch shown in Fig. 7 (and identified by reference numeral 708) is not depicted in each of Figs. 9 and 10, only to simplify those drawings. However, it is to be understood that such an access mechanism is or can be coupled to each of the controllers 906 and 1006 of Figs. 9 and 10, respectively.

Again, in a security system 900 or 1000, a smartcard reader may be setup to give access on a per door basis or to equipment. In general, the smartcard reader communicates with the smartcard and information is read from the smartcard for access, information is sent to the controller, and the controller determines whether or not to grant access and activates an access mechanism if granted. Secure transmission from a smartcard reader is provided by encrypting the messages from the smartcard reader in the security system. Preferably, the smartcard reader is a biometrics smartcard reader 500/600, but ordinary smartcard readers may be practiced.

The system 900 of Fig. 9 comprises a smartcard reader 902, a high security module (HSM) 904, and an access controller 906. While not shown in Fig. 9 to simplify the drawing, the controller 906 may be coupled to an access mechanism able to provide access (e.g., to a door, portal, computer, network, or other secure equipment or installation) at an access point. Preferably, the smartcard reader is a biometrics smartcard reader 500/600, but ordinary smartcard readers may be practiced. The smartcard reader may be a Banque-Tec International reader.

A smartcard 920 (e.g., a Mifare smartcard) is presented to the smartcard reader 902, and the smartcard reader 902 communicates with the smartcard. Preferably, communications between the Mifare smartcard 920 and the smartcard reader 902 are encrypted using Mifare proprietary encryption. However, other forms of encryption may be practiced without departing from the scope and spirit of the invention. The description accompanying Fig. 10 provides examples of other encryption techniques that may be practiced. Also, the smartcard 920 preferably includes biometrics data, as described hereinbefore. The reader 902 reads access information from the smartcard 920. The access information may include one or more of the following: person's name, facility code, company code, access code, and issue code. Other access information and/or authorisation data may be sent from the smartcard reader 902 to the HSM 904 using suitable communications protocols, such as RS232 or RS485. Other communications protocols may be practiced without departing from the scope and spirit of the invention.

The HSM 904 is located remotely from the smartcard reader 902 and preferably at an inaccessible location relative to the smartcard reader 902. Communications between the reader 902 and the HSM 904 are encrypted. The encryption technique used may use one or more of the following techniques: Triple DES (3DES), Skipjack, and AES-Rijndael. Other encryption techniques may be practiced without departing from the scope and spirit of the invention. The distance between the smartcard reader 902 and the HSM 904 may be up to at least 1.2 kilometres, e.g. if RS485 is used. The distance between the smartcard reader 902 and the HSM 904 may be varied dependent on the communications protocol, techniques, and media used.

The HSM 904 is in turn coupled to a controller 906. Communications between the HSM 904 and the controller 906 are carried out using the controller-specified format, which is usually Wiegand format but may be another format (e.g., clock and data). The distance between the HSM 904 and the controller 906 may be up to 500 feet. However, this distance may be varied without departing from the scope and spirit of the invention. In turn, the controller 906 may be connected to an access point (e.g., the door latch 708 of Fig. 7) to control operation of the access point. Different access mechanisms may be used.

The HSM 904 translates the encrypted signal to another format for a controller and communicates the translated signal to the access controller 906. The translation preferably involves decrypting the message to obtain the security or access information from the smartcard, e.g. "Facility Code" and the "Access number" and communicating the values to the access controller. Thus, communications between the smartcard reader 902 and the HSM 904 and thus the controller 906 is secure whether the smartcard reader 902 is removed from the wall or wiring is accessed through a wall. This provides a higher standard of security for access control systems. The process of Fig. 8 applies to this embodiment.

The system 1000 of Fig. 10 comprises a smartcard reader 1002, a high security module (HSM) 1004, and an access controller 1006. While not shown in Fig. 10 to simplify the drawing, the controller 1006 may be coupled to an access mechanism (e.g., to a door, portal, computer, network, or other secure equipment or installation) at an access point. Preferably, the smartcard reader is a biometrics smartcard reader 500/600, but ordinary smartcard readers may be practiced. The smartcard reader may be a Banque-Tec International reader. The system of Fig. 10 is largely identical to that of Fig. 9 and therefore the following description is limited to identifying the points of difference for the sake of brevity.

A smartcard 1020 (e.g., a DESFIRE Mifare smartcard) is presented to the smartcard reader 1002, and the smartcard reader 1002 communicates with the smartcard. Preferably, communications between the Mifare smartcard 1020 and the smartcard reader 1002 are encrypted using triple DES (3DES) encryption. However, other forms of encryption may be practiced without departing from the scope and spirit of the invention. The remainder of the system 1000 is the same as that for the system 900 of Fig. 9, and is not repeated for the sake of brevity. The process of Fig. 8 applies to this embodiment.

A small number of embodiments of the invention regarding methods, devices, and systems for biometric smartcard reading and encoding, as well as for secure transmissions have been described. In the light of the foregoing, it will be apparent to

those skilled in the art in the light of this disclosure that various modifications may be made without departing from the scope and spirit of the invention.

Claims

The claims defining the invention are as follows:

1. A method of providing secure transmissions from a smartcard reader, said method comprising the steps of:

encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information;

transmitting said encrypted signal to a remote location relative to said smartcard reader;

translating at said remote location said transmitted signal to another format useable by an access controller; and

controlling an access mechanism using said access controller dependent upon said translated signal.

2. The method according to claim 1, wherein said smartcard contains biometric data and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly.

3. The method according to claim 2, wherein said biometric data comprises fingerprint data.

4. The method according to claim 2 or 3, wherein said biometric data is not transmitted to said remote location from said smartcard reader.

5. The method according to claim 1, further comprising the step of providing access using said access mechanism if said translated signal is determined by said access controller to authorise access.

6. The method according to claim 5, wherein said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation.

7. The method according to any one of claims 1-5, wherein said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code.

8. The method according to any one of claims 1-7, wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

9. The method according to claim 1, further comprising the step of encrypting communications between said smartcard and said smartcard reader.

10. The method according to any one of claims 1-9, wherein said encrypted signal is transmitted from said smartcard reader to a high security module at said remote location.

11. The method according to claim 10, wherein said high security module translates said encrypted signal to said other format.

12. The method according to claim 10, wherein said smartcard reader and said high security module are separated by a distance of up to 1.2 kilometres.

13. The method according to claim 10, wherein said smartcard reader and said high security module are separated by a distance of up to 15 metres.

14. The method according to any one of claims 1-13, wherein said translated signal is in a controller-specified format.

15. The method according to claim 14, wherein said controller-specified format is Wiegand format, or clock and data.

16. A system for providing secure transmissions from a smartcard reader, said system comprising:

a smartcard reader for encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information, and for transmitting said encrypted signal to a remote location relative to said smartcard reader;

a high security module for receiving said transmitted signal and translating said transmitted signal to another format useable by an access controller; and

an access controller for controlling an access mechanism using said access controller dependent upon said translated signal.

17. The system according to claim 16, wherein said smartcard contains biometric data, and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly.

18. The system according to claim 17, wherein said biometric data comprises fingerprint data.

19. The system according to claim 17 or 18, wherein said biometric data is not transmitted to said high security module from said smartcard reader.

20. The system according to claim 16, further comprising an access mechanism providing access if said translated signal is determined by said access controller to authorise access.

21. The system according to claim 20, wherein said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation.

22. The system according to any one of claims 16-21, wherein said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code.

23. The system according to any one of claims 16-22, wherein said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption.

24. The system according to claim 16, wherein communications between said smartcard and said smartcard reader are encrypted.

25. The system according to claim 24, wherein said smartcard reader and said high security module are separated by a distance of up to 1.2 kilometres.

26. The system according to claim 24, wherein said smartcard reader and said high security module are separated by a distance of up to 15 metres.

27. The system according to any one of claims 16-26, wherein said translated signal is in a controller-specified format.

28. The system according to claim 27, wherein said controller-specified format is Wiegand format, or clock and data.

29. An apparatus for providing secure transmissions from a smartcard reader, said apparatus comprising:

a smartcard reader for encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information;

means for transmitting said encrypted signal to a remote location relative to said smartcard reader;

means for translating at said remote location said transmitted signal to another format useable by an access controller; and

an access controller for controlling an access mechanism dependent upon said translated signal.

30. The apparatus according to claim 29, wherein said smartcard contains biometric data and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly.

31. The apparatus according to claim 30, wherein said biometric data comprises fingerprint data.

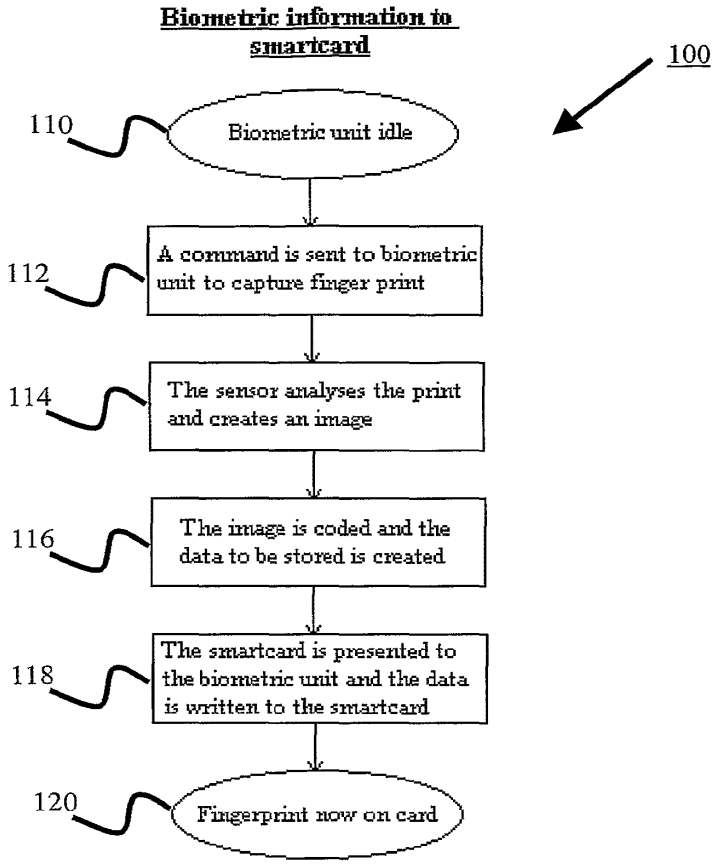

Biometric information to smartcard
100
110
Biometric unit idle
112
A command is sent to biometric unit to capture finger print
114
The sensor analyses the print and creates an image
116
The image is coded and the data to be stored is created
118
The smartcard is presented to the biometric unit and the data is written to the smartcard
120
Fingerprint now on card

FIG. 1

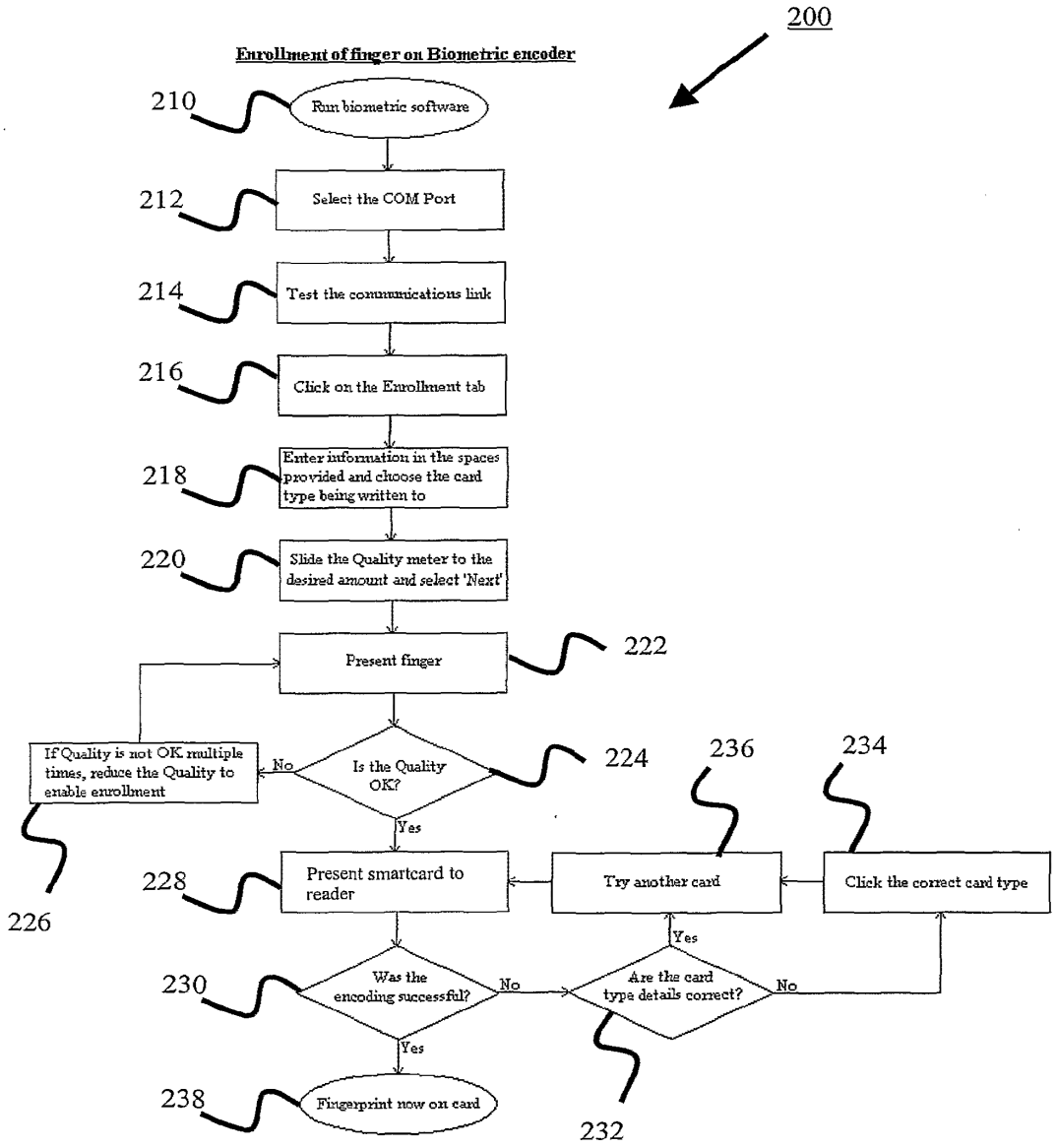

200
Enrollment of finger on Biometric encoder
210
Run biometric software
212
Select the COM Port
214
Test the communications link
216
Click on the Enrollment tab
218
Enter information in the spaces provided and choose the card type being written to
220
Slide the Quality meter to the desired amount and select 'Next'
Present finger
222
If Quality is not OK multiple times, reduce the Quality to enable enrollment
No
Is the Quality OK?
224
Yes
226
228
Present smartcard to reader
Try another card
236
Click the correct card type
234
Yes
230
Was the encoding successful?
No
Are the card type details correct?
No
Yes
232
238
Fingerprint now on card

FIG. 2

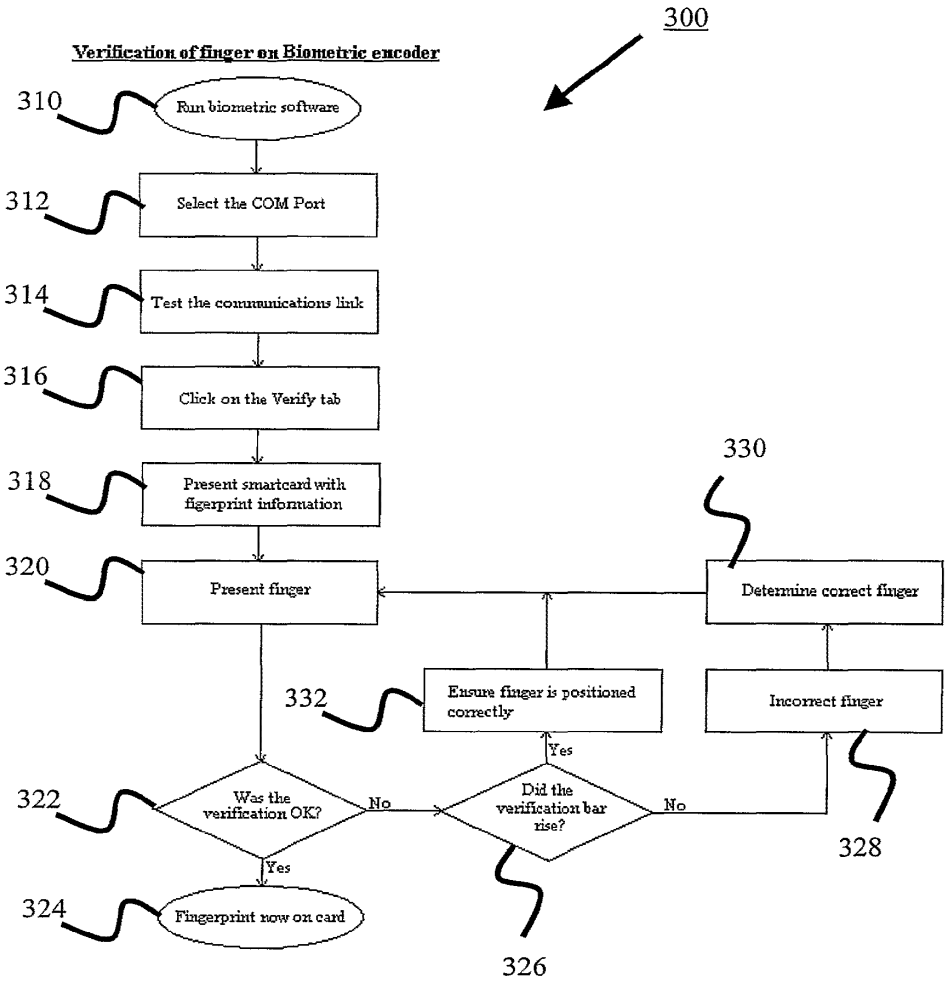

300
Verification of finger on Biometric encoder
310
Run biometric software
312
Select the COM Port
314
Test the communications link
316
Click on the Verify tab
318
Present smartcard with fingerprint information
320
Present finger
330
Determine correct finger
332
Ensure finger is positioned correctly
Incorrect finger
Yes
322
Was the verification OK?
No
Did the verification bar rise?
No
328
Yes
324
Fingerprint now on card
326

FIG. 3

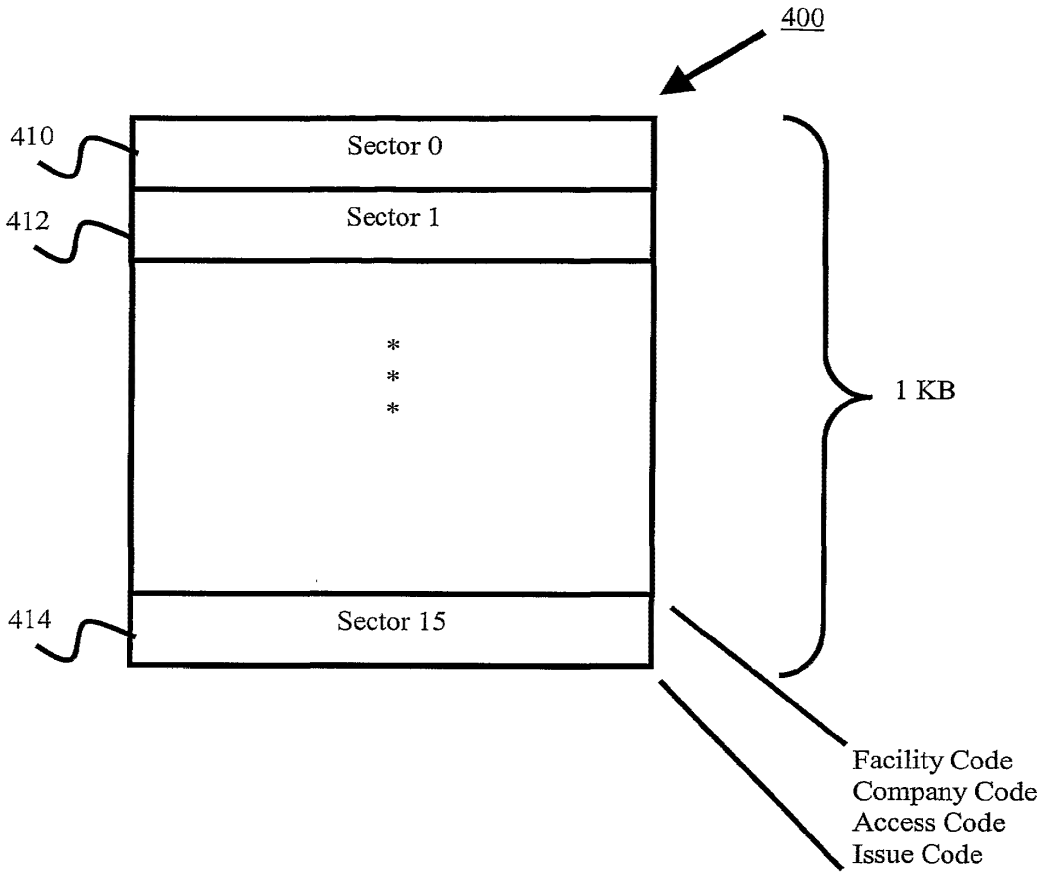


FIG. 4A

Sector	Key A	Key B
0	A0A1A2A3A4 or FFFFFFFFFF	- -
*		
*		
*		
15		

450

FIG. 4B

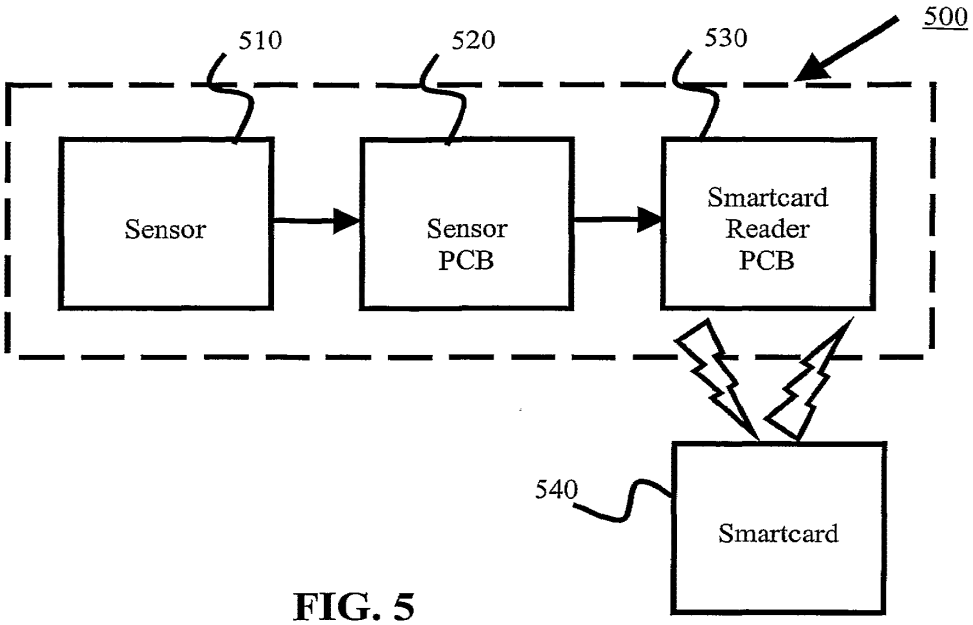

500
510
520
530
Sensor
Sensor PCB
Smartcard Reader PCB
540
Smartcard

FIG. 5

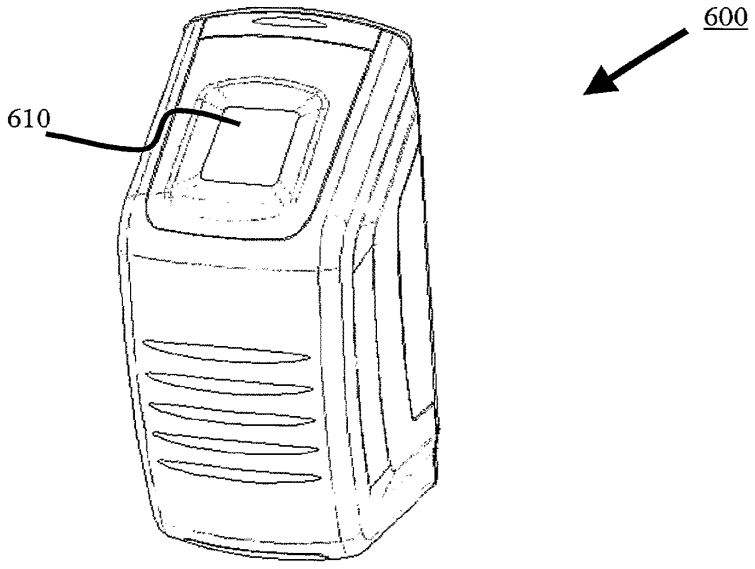

600
610

FIG. 6

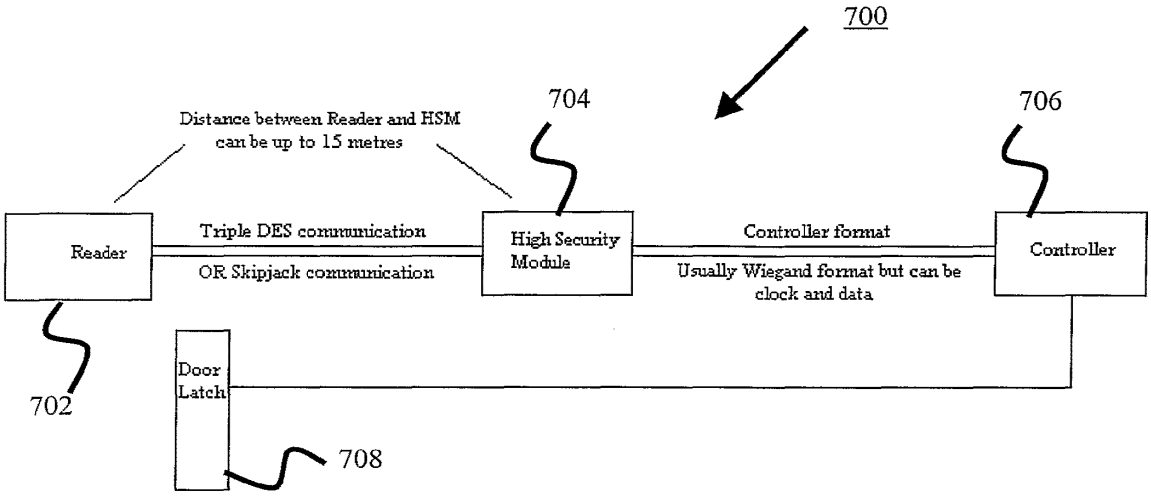

700
704
706
Distance between Reader and HSM
can be up to 15 metres
Reader
Triple DES communication
OR Skipjack communication
High Security
Module
Controller format
Usually Wiegand format but can be
clock and data
Controller
Door
Latch
702
708

FIG. 7

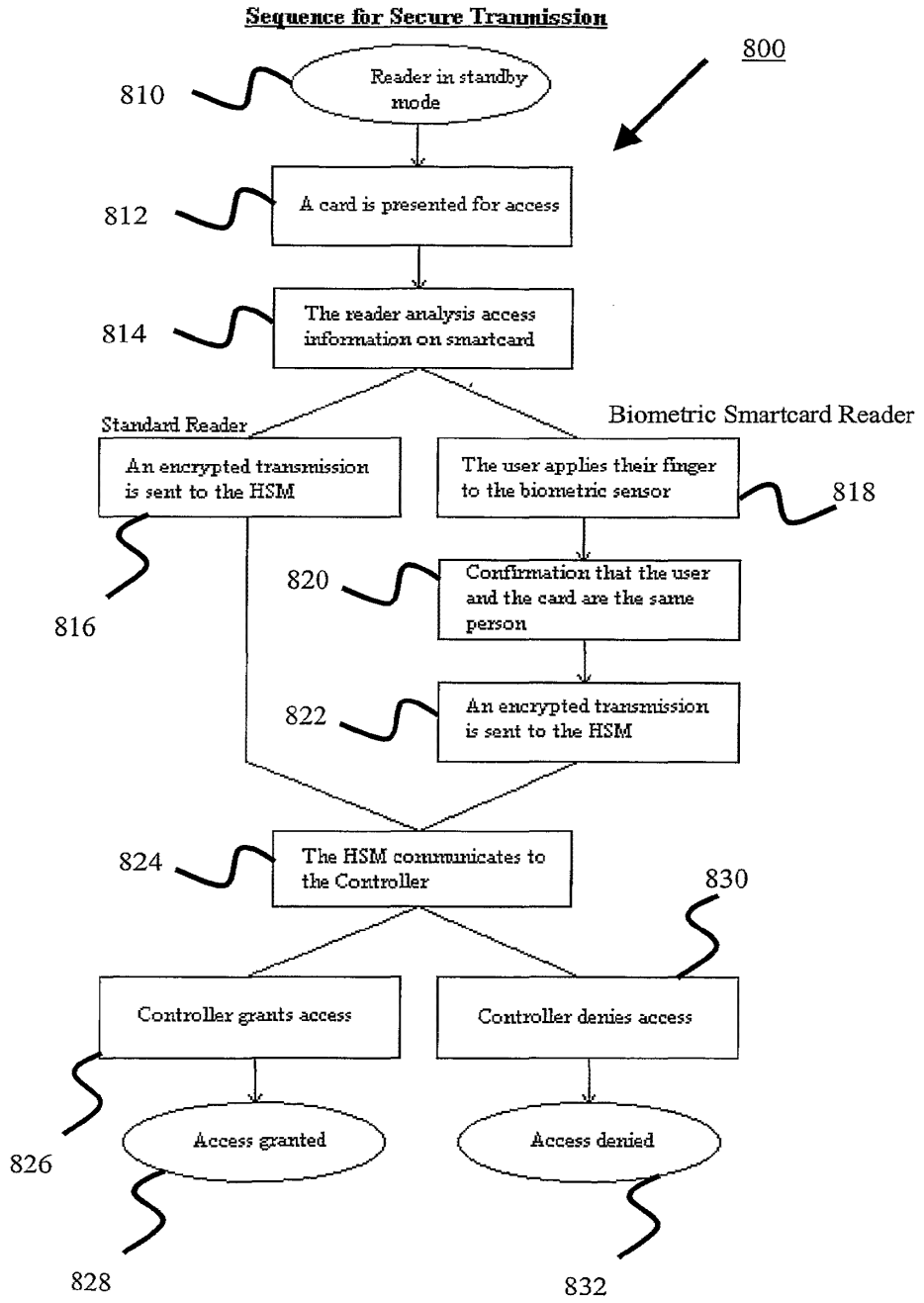

Sequence for Secure Transmission
800
810
Reader in standby mode
812
A card is presented for access
814
The reader analysis access information on smartcard
Standard Reader
Biometric Smartcard Reader
An encrypted transmission is sent to the HSM
The user applies their finger to the biometric sensor
818
816
820
Confirmation that the user and the card are the same person
822
An encrypted transmission is sent to the HSM
824
The HSM communicates to the Controller
830
Controller grants access
Controller denies access
826
Access granted
Access denied
828
832

FIG. 8

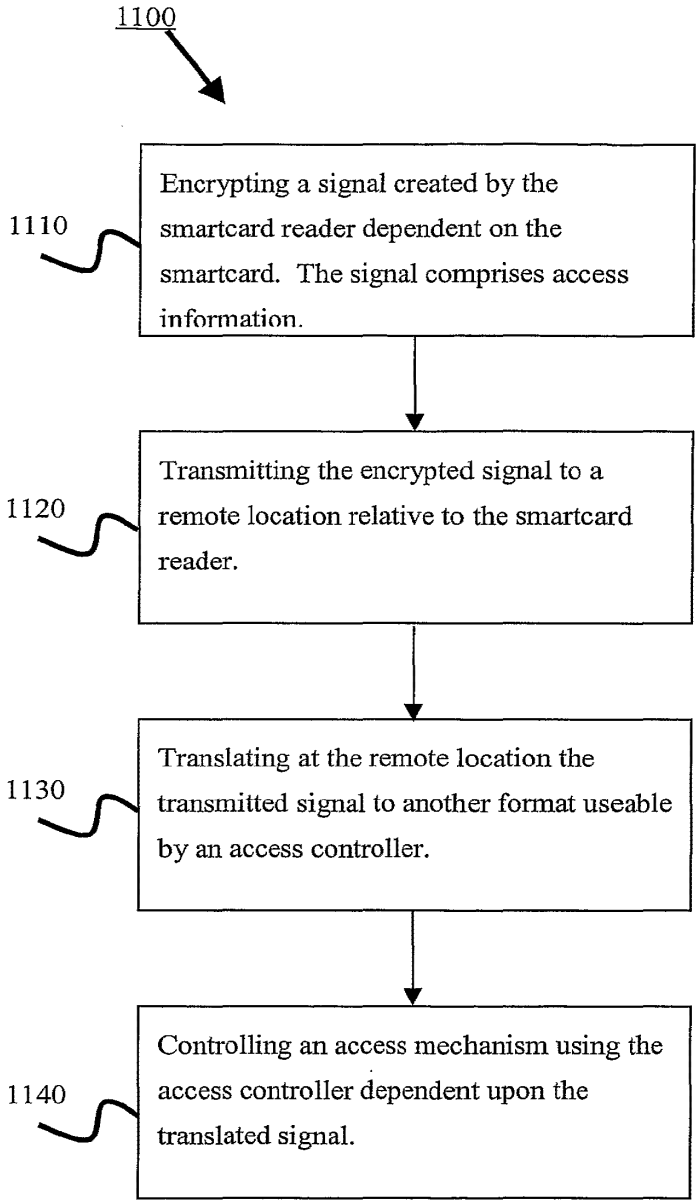

1100
1110
Encrypting a signal created by the smartcard reader dependent on the smartcard. The signal comprises access information.
1120
Transmitting the encrypted signal to a remote location relative to the smartcard reader.
1130
Translating at the remote location the transmitted signal to another format useable by an access controller.
1140
Controlling an access mechanism using the access controller dependent upon the translated signal.

Fig. 11

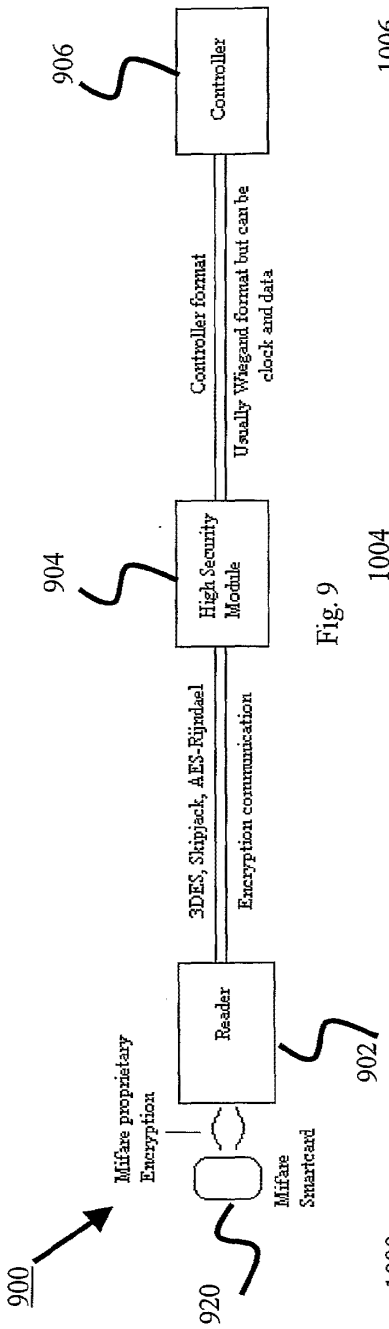

900
Mifare proprietary Encryption
920
Mifare Smartcard
Reader
902
3DES, Skipjack, AES-Rijndael
Encryption communication
High Security Module
904
Controller format
Usually Wiegand format but can be clock and data
Controller
906

Fig. 9

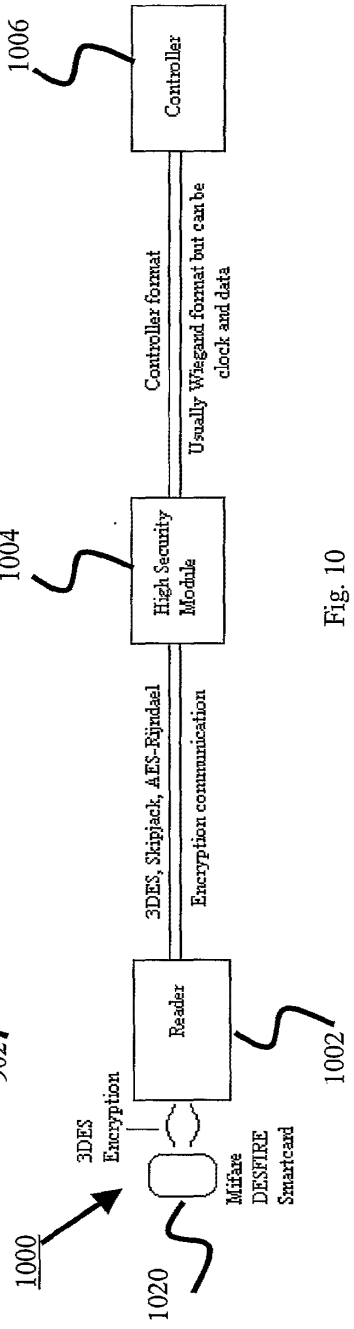

1000
3DES Encryption
1020
Mifare DESFIRE Smartcard
Reader
1002
3DES, Skipjack, AES-Rijndael
Encryption communication
High Security Module
1004
Controller format
Usually Wiegand format but can be clock and data
Controller
1006

Fig. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/00934

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06K 019/07

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DWPI, USPTO (SMARTCARD, ENCRYPT, REMOTE ETC)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5995965 (EXPERTON) 30 November 1999 Column 4, lines 9 to 26 Column 5, lines 50 to 56 Column 10, lines 21 to 33	1, 5 - 7, 29
X	US 5991410 (ALBERT ET AL) 23 November 1999 Column 5, lines 18 - 20 Column 18, lines 45 - 62	1, 5 - 9, 29 - 31

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 August 2003	-1 SEP 2003
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **M.J. O'ROURKE** Telephone No : (02) 6283 2017

WAVELYNX EX. 1003, Pg. 1836
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/00934

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6366967 B1 (WAGNER) 2 April 2002 Column 6, lines 11 - 63	1, 5 - 9, 29 - 31
X,P	JP 2002-261749 A (MATSUSHITA ELECTRIC IND CO LTD) 13 September 2002 Paragraph 0010 - 0013 of english translation from Detailed Description (online), (Retreived on 7 August 2003) Retrieved from the Internet < URL: http://www6.ipdl.jpo.go.jp/Tokujitu/PAJdetail.ipdl?N0000=80&N0120=01&N2001=2&N3001=2002-261749>	1 - 9, 14 - 15, 29 - 31

WAVELYNX EX. 1003, Pg. 1837
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU03/00934

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	5995965	NONE					
US	5991410	US	2002030579				
US	6366967	US	5742845	US	5905908	US	2002032810
		US	2002138430	US	2002198837	US	5898838
JP	2002261749	NONE					

END OF ANNEX

WAVELYNX EX. 1003, Pg. 1838
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2005 (06.01.2005)

PCT

(10) International Publication Number
WO 2005/001777 A1

(51) International Patent Classification[7]: G07C 9/00

(21) International Application Number:
PCT/US2004/016616

(22) International Filing Date: 16 June 2004 (16.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
203 09 254.6 16 June 2003 (16.06.2003) DE

(71) Applicant *(for all designated States except US)*: **SCM MICROSYSTEMS GMBH** [DE/DE]; Oskar-Messter-Strasse 13, 85737 Ismaning (DE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MERKERT, Robert, J., Sr.** [US/US]; 21 Chippenham Drive, Voorhees, NJ 08043 (US).

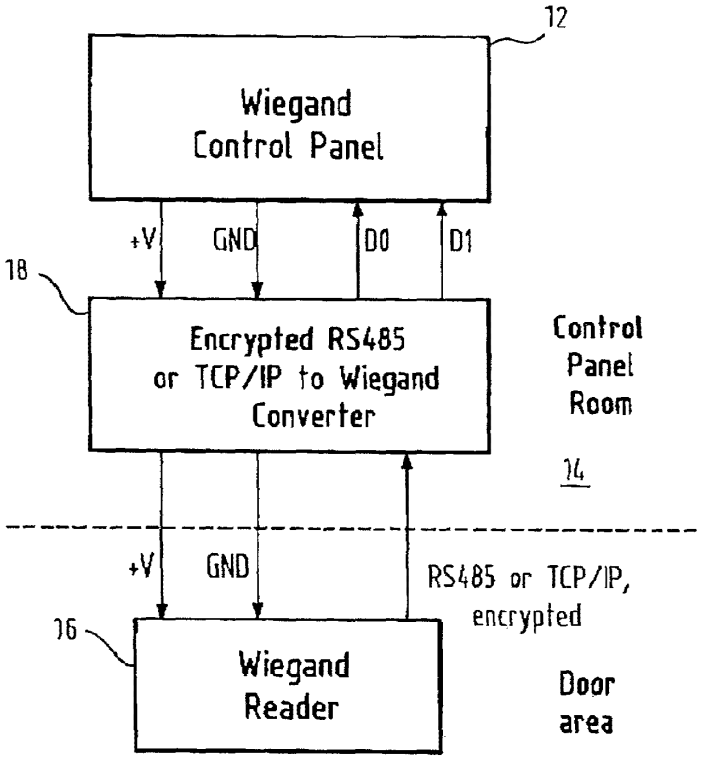
(74) Agent: **GARRETT, Arthur, S.**; Finnegan, Henderson, Farrabow Garrett & Dunner, L.L.P., 1300 I Street, NW, Washington, DC 20005-3315 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

[Continued on next page]

(54) Title: ACCESS SYSTEM



(57) Abstract: An access system includes an input device which is accessible to a user and capable of reading an authentication and/or identification information provided by the user. The access system further includes a Wiegand control panel (12) connected to the input device for evaluation of the information provided by the user. The control panel (12) is located in a secure area (14) remote from the input device. The access system further includes a converter (18) connected to the input device and to the control panel (12). The input device includes encryption means to encrypt the information provided by the user. The converter (18) is capable of converting the encrypted information into a standard Wiegand signal.

WO 2005/001777 A1

WAVELYNX EX. 1003, Pg. 1839
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ACCESS SYSTEM

DESCRIPTION OF THE INVENTION

This application claims the right to foreign priority based on German Patent Application No. 203 09 254:6, entitled "ACCESS SYSTEM," filed in the Federal Republic of Germany, on June 16, 2003, which is hereby incorporated herein by reference.

The invention relates to an access system, comprising an input device which is accessible to a user and capable of reading an authentication and/or identification information provided by the user, and a Wiegand control panel connected to the input device for evaluation of the information provided by the user, the control panel being located in a secure area remote from the input device.

Security systems using Wiegand readers and control panels adapted to evaluate the data read from a Wiegand card are well known and widely employed in various applications like systems for unlocking doors or parking garage gates etc. Usually, the Wiegand reader is located to be accessible to the user (Wiegand card holder) while the control panel, which after a positive evaluation of the data perform a security relevant operation (e.g. unlocking a door) is located in an area which is not accessible to the user, e.g. in a closed room, to guarantee a certain level of security.

US-5 679 945 shows an access system of the type mentioned in the beginning which provides an "intelligent" card reader in order to replace existing magnetic stripe readers, bar code readers and Wiegand readers without the need for retrofitting of existing computer systems which are coupled to the existing readers.

The invention provides an access system with an extremely high level of security.

This object of the invention is attained with a security system of the type mentioned in the beginning wherein the access system further comprises a converter connected to the input device and to the control panel, the input device comprising encryption means to encrypt the information provided by the user, and the converter being capable of converting the encrypted

WAVELYNX EX. 1003, Pg. 1841
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

information into a standard Wiegand signal. Thus, the access system provides a higher level of security because the data read from the input device is transferred in an encrypted form. Moreover, the system offers more flexibility because it is not limited to Wiegand readers as input devices, while the existing Wiegand control panels can still be used.

Preferably the converter is co-located with the control panel in the secure area. In this configuration there is no chance to intercept and abuse the information.

This guarantees an even higher security with regard to the data transfer from the input device to the control panel because it is not possible to intercept and abuse the authentication/identification information provided by the user since the information is encrypted until it reaches the converter which, together with the control panel, is located in the secure area which is not accessible to a fraud. In other words, a secure communication channel between the input device and the securely located converter is provided.

The input device preferably comprises a smart card reader into which a secure output can be implemented, for example a RS485 or a TCP/IP output.

According to a preferred embodiment of the invention the access system further comprises a host computer connected to and located remote from the input device. Preferably, the host computer is also connected to the control panel and the data between the input device and the host computer is transmitted using a RS485 or a TCP/IP protocol.

Thus, the remote host computer may be an existing access control system host computer which, after a slight modification and/or addition to the system software, can be used to configure and to control the input device in a secure manner.

BRIEF DESCRIPTION OF THE DRAWINGS

Further details of the invention become apparent from the following description in connection with the accompanying drawings. In the drawings:

Fig. 1 shows an access system according to the prior art.

Fig. 2 shows an access system according to an embodiment of the invention.

WAVELYNX EX. 1003, Pg. 1842
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Fig. 3 shows an enhanced access system according to a further embodiment of the invention.

The prior art access system illustrated in Fig. 1 includes a standard Wiegand reader 10 and a Wiegand control panel 12 adapted to retrieve data from a standard Wiegand reader. The control panel 12 is located in a secure area 14 remote from the Wiegand reader 10, which is accessible to a user. In order to gain access the user ins his Wiegand card (not shown), which contains authentication and, if required identification information, into the Wiegand reader 10. The information is transmitted from the reader 10 to the control panel 12 where the information is evaluated. Depending on the result of the evaluation the control panel 12 either perform a security relevant operation, e.g. unlocking a door or the like, to grant the user the requested access, or it denies such operation.

The embodiment of the invention shown in Fig. 2 also makes use of a Wiegand control panel 12. (It has to be understood that the term "Wiegand control panel" is not restricted to a particular hardware configuration but rather includes any suitable control panel which is capable of processing signals/data in a Wiegand format by using corresponding software.) However, the standard Wiegand reader is replaced by another input device, in particular a smart card reader 16 into which a smart card (not shown) containing the authentication/identification information can be inserted. The smart card reader 16 includes means for encrypting the information stored on the smart card and an RS485 or TCP/IP output. The access system according to the invention further comprises a converter 18 connected both to the smart card reader 16 and to the control p el 12. The converter 8 and the control panel 12 are co-located in a secure area 14 remote from the smart card reader 16 and have a direct interface connection.

The operation of the access system of Fig. 1 will now be described. The user inserts his smart card into the smart card reader 16. The information on the smart card is read and encrypted by the encryption means of the smart card reader 16. The encrypted information is transmitted to the converter 18 using a secure RS485 or TCP/IP protocol. Thus, the connection

WAVELYNX EX. 1003, Pg. 1843
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

between the smart card reader 16 and the converter 18 can be regarded as a "secure channel". The converter 18 converts the encrypted information into a standard Wiegand signal and sends it to the control panel 12. The control panel 12 is able to evaluate the Wiegand signal and decide whether to allow or to deny access.

Fig. 3 depicts a further embodiment of the invention which has substantially the same configuration as the embodiment of Fig. 2, but further includes a remote host computer 20 which is connected both to the input device, preferably a smart card reader 16, and to the control panel 12. The host computer 20 is located outside the secure area 14 of the control panel 12 and the converter 18. The communication between the host computer 20 and the smart card reader 16 is provided by a further secure channel, i.e. data is transferred using an RS485 or a TCP/IP protocol.

The operation of the access system of Fig. 3 to gain access is the same as described above. However, the access system can easily be adapted to various requirements. For example, the secure channel between the remote host computer 20 and the smart card reader 16 is be used to change the configuration of the smart card reader 16 on command from the host computer 20 in a comfortable and secure manner. Moreover, the host computer 20 can be used to define the type of input device that is required to gain access. Suitable input devices include contactless smart card reader, contact smart card reader, PIN pad, biometric device (e.g. fingerprint reader) and combinations thereof. The input devices required can be changed as a function of security threat level, day of week, time of day, or other conditions. The connection between the host computer 20 and the control panel 12 allows to check whether a control panel operation has been successfully executed. Further, the host computer 20 can be used to identify a possible malfunction of the control panel 12 by using test signals.

It has to be understood that the invention is not limited to embodiments using an RS485 or TCP/IP protocol. The communication through the secure channels may be provided by any other suitable protocol.

WAVELYNX EX. 1003, Pg. 1844
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

WHAT IS CLAIMED IS:

1. An access system, comprising an input device which is accessible to a user and capable of reading an authentication and/or identification information provided by the user, and a Wiegand control panel (12) connected to the input device for evaluation of the information provided by the user, the control panel (12) being located in a secure area (14) remote from the input device, characterized in that the access system further comprises a converter (18) connected to the input device and to the control panel (12), the input device comprising encryption means to encrypt the information provided by the user, and the converter (18) being capable of converting the encrypted information into a standard Wiegand signal.

2. The access system according to claim 1, characterized in that the converter (18) is co-located with the control panel (12) in the secure area (14).

3. The access system according to claim 1, characterized in that the input device comprises a smart card reader (16).

4. The access system according to claim 1, characterized in that the input device comprises at least one of a PIN pad and a biometric device.

5. The access system according to claim 1, characterized in that the encrypted information is transmitted from the input device to the converter (18) using one of a RS485 and a TCP/IP protocol

6. The access system according to claim 1, characterized in that the access system further comprises a host computer (20) connected to and located remote from the input device.

7. The access system according to claim 5, characterized in that the host computer (20) is also connected to the control panel (12).

8. The access system according to claim 7, characterized in that the data between the input device and the host computer (20) is transmitted using one of a RS485 and a TCP/IP protocol.

WAVELYNX EX. 1003, Pg. 1845
WaveLynx Technologies v. ASSA Abloy, IPR2023-01018

Fig. 2

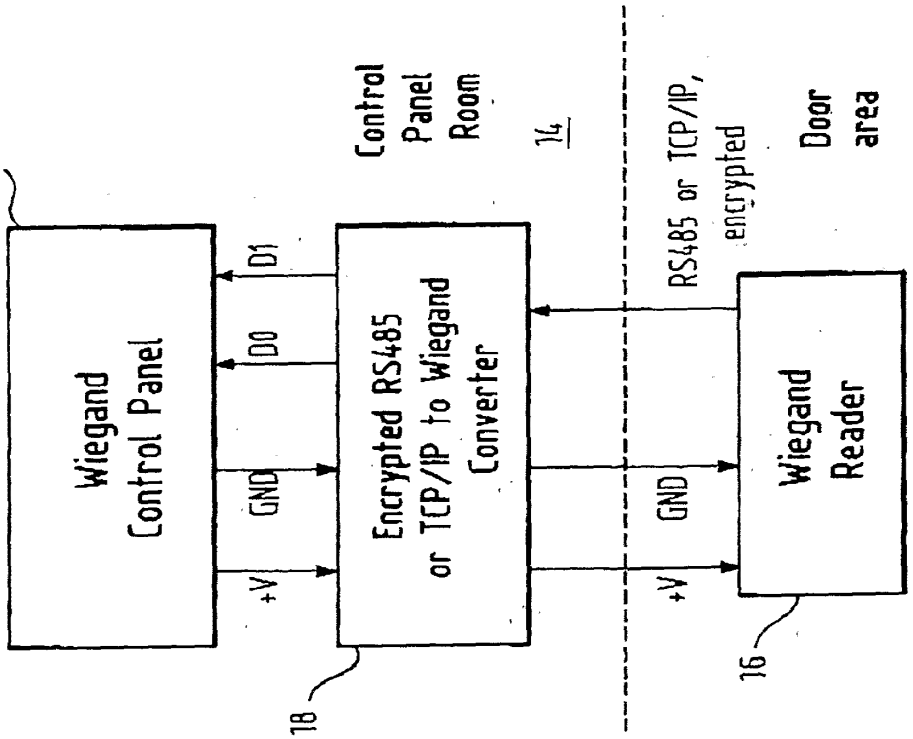
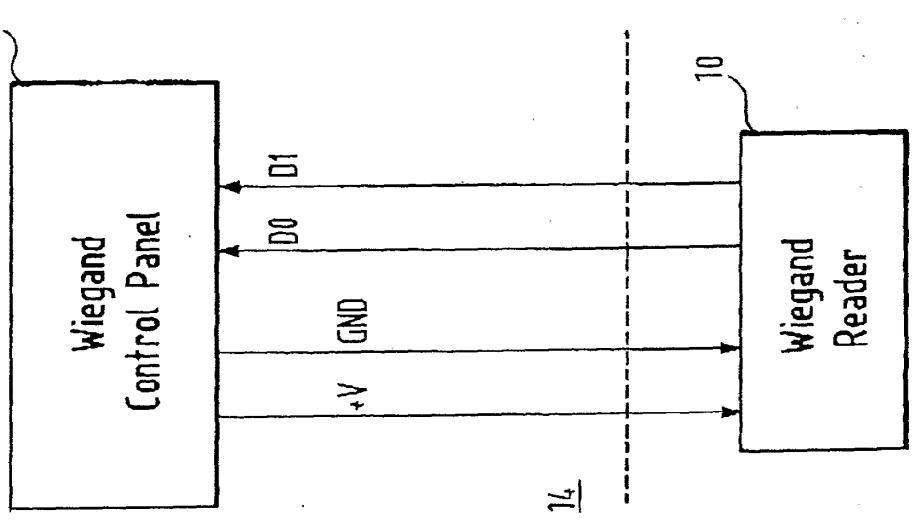

12
Wiegand Control Panel
D1
D0
GND
+V
Control Panel Room
14
Encrypted RS485 or TCP/IP to Wiegand Converter
18
RS485 or TCP/IP, encrypted
Door area
GND
+V
Wiegand Reader
16

Fig. 1


12
Wiegand Control Panel
D1
D0
GND
+V
14
10
Wiegand Reader

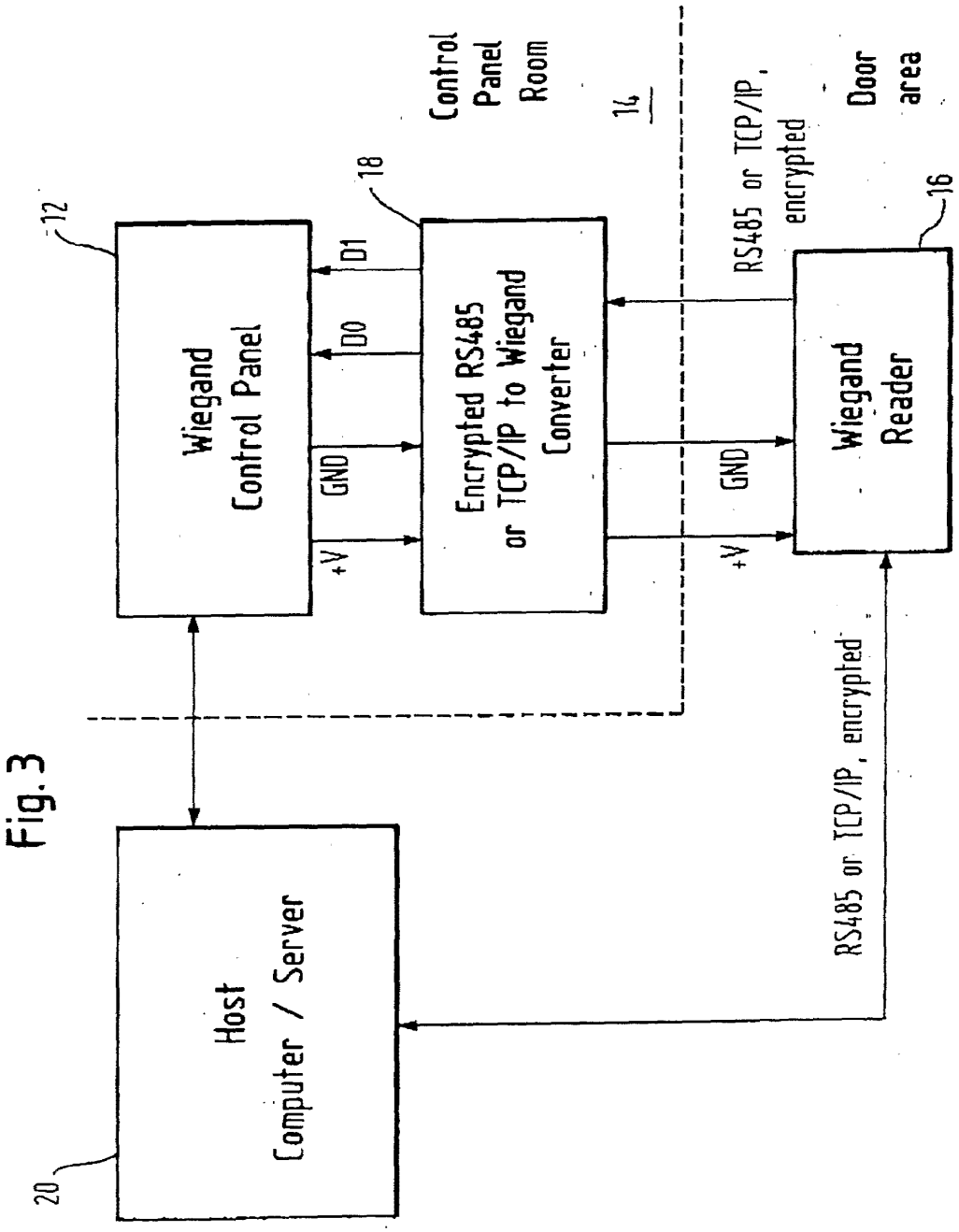

Control Panel Room
14
Door area
12
Wiegand Control Panel
18
Encrypted RS485 or TCP/IP to Wiegand Converter
16
Wiegand Reader
D1
D0
GND
+V
RS485 or TCP/IP, encrypted
GND
+V
RS485 or TCP/IP, encrypted
Host Computer / Server
20

Fig. 3