I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY: Elizabeth A. McGrath

DATE: 7/21/98

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re:	Patent Application of Leon Stambler	: Group Art Unit: 2735
Appln. No.:	08/872,116	: Examiner: B. Zimmerman
Filed:	June 10, 1997	:
For:	METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION (as amended)	: Attorney Docket No. 6074-107

AMENDMENT

This amendment is in response to the Office Action mailed April 22, 1998, and is being timely filed within the three (3) month shortened statutory period set for response therein.

No extension of time fee is believed to be due for filing this paper. However, if any extension of time fee is due, charge the fee to Deposit Account No. 16-0235. A separate sheet is enclosed for payment of the fee for presenting extra claims.

Please amend the above-identified application as follows, without prejudice:

In the Claims:

Cancel claims 64-66, 68-71, 73-75, 77-86, 99-107 and 109.

Amend claim 87 as follows:

~~87.~~ **(Amended)** A method for coding clear information comprising [the steps of]:

receiving a personal identification number (PIN) from an originator;

[deriving] obtaining first coded authentication information by using the PIN;

generating at least two numbers using the first coded authentication information, at least one of the at least two numbers being an arbitrary number;

storing the at least two numbers in at least one storage means; and

coding the clear information [with] using the first coded authentication information to derive coded information.

Amend claim 88 as follows:

~~88.~~ **(Amended)** The method of claim ~~87~~ wherein the coded information is uncoded using second coded authentication information to recover the clear information, the method further comprising [the steps of]:

retrieving the at least two numbers stored in the at least one storage means;

combining the retrieved at least two numbers to derive the second coded authentication information; and

uncoding the coded information using the derived second coded authentication information to recover the clear information.

Amend claim 92 as follows:

~~92.~~ 6 **(Twice Amended)** A method for securing the integrity of first information relevant to a transaction, and the integrity of second information associated with at least an originator party, by using a variable authentication number (VAN), the first information including a transaction sequence number which is previously stored in a storage means and is revised for each transaction, the method comprising [the steps of]:

coding the first information [with] <u>using</u> at least the second information to derive the VAN;

appending the VAN to the first information;

retrieving the transaction sequence number from the storage means;

uncoding the VAN to recover the first information including the transaction sequence number by using at least third information associated with the originator party; and

authenticating the integrity of the first and second information by comparing the recovered transaction sequence number with the retrieved transaction sequence number.

Amend claim 95 as follows:

~~95.~~ 9 6 **(Amended)** The method of claim ~~92~~ wherein at least selected portions of the first information are coded to derive a compact error detection code, the compact error detection code

being further coded [with] using at least the second information to derive a compact VAN which is used to detect changes in at least the first information and at least the second information.

Amend claim 108 as follows:

~~108.~~ **(Amended)** A method for authenticating the integrity of first transaction information and second transaction information, and a first party associated with the first and second transaction information, the integrity of the first and second transaction information being authenticated with a variable authentication number (VAN), the method comprising [the steps of]:

coding the first transaction information to generate a first error detection code (EDC1);

coding the second transaction information to generate a second error detection code (EDC2);

coding, or otherwise combining, EDC1 and EDC2 to generate a third error detection code (EDC3);

coding EDC3 and first information associated with the first party to derive the variable authentication number (VAN);

associating the VAN and EDC2 with the first transaction information to form a first information group;

associating the VAN and EDC1 with the second transaction information to form a second information group; and

subsequently authenticating the integrity of the first transaction information, and the second transaction information by [performing the steps of]:

recovering the VAN from the first information group, and uncoding the recovered VAN by using second information

associated with the first party to derive the third error detection code (EDC3);

recovering the first transaction information from the first information group, and coding the recovered first transaction information to generate a fourth error detection code (EDC4);

recovering the EDC2 from the first information group, and coding, or otherwise combining, EDC4 and the recovered EDC2 to generate a sixth error detection code (EDC6);

authenticating the integrity of the first transaction information if EDC6 compares favorably with the EDC3 recovered from the VAN;

recovering the VAN from the second information group, and uncoding the recovered VAN by using second information associated with the first party to derive the third error detection code (EDC3);

recovering the second transaction information from the second information group, and coding the recovered second transaction information to generate a fifth error detection code (EDC5);

recovering the EDC1 from the second information group, and coding, or otherwise combining, the recovered EDC1 and EDC5 to generate a seventh error detection code (EDC7); and

authenticating the integrity of the second [tranaction] transaction information if EDC7 compares favorably with the EDC3 recovered from the VAN.

Add new claims 110-150 as follows:

14
--~~110~~. In a multi-party transaction system, a method for securing information relevant to a transaction by using information associated with a present party and information associated with an absent party, wherein a credential is previously issued to at least one of the present party and the absent party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:

creating the VAN by coding credential information with a secret key of the credential issuing entity;

authenticating at least one of the present party and the absent party by using the VAN; and

coding the information relevant to the transaction using the information associated with the present party, and then coding the result using the information associated with the absent party.

15 14
~~111~~. The method of claim ~~110~~ wherein the information associated with the present party or the absent party includes personal key, the method further comprising:

using the credential issuing entity to create the personal key, and including the personal key in the credential information.

16 15
~~112~~. The method of claim ~~111~~ further comprising:

the credential issuing entity previously verifying that the personal key is unused by another party.

17 14
~~113~~. The method of claim ~~110~~ further comprising:

uncoding the coded information relevant to the transaction using information associated with the absent party and using information associated with the present party to recover the relevant transaction information.

18 14
~~114~~. The method of claim ~~110~~ wherein the information relevant to the transaction comprises coded or non-coded information.

19 14
~~115~~. The method of claim ~~110~~ wherein the credential information further includes secret information associated with the present or absent party only if a predetermined personal identification number (PIN), or password, or other personal information or characteristic is used by the present or absent party to access the secret information.

20
~~116~~. In a multi-party transaction system, a method for securing information relevant to a transaction by using information associated with at least two parties, wherein a credential is previously issued to at least one of the parties by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:

creating the VAN by coding credential information with a secret key of the credential issuing entity;

authenticating at least one of the parties by using the VAN;

coding information associated with the at least two parties to generate a joint code; and

coding the information relevant to the transaction with the joint code to generate coded information relevant to the transaction.

21 ~~117.~~ The method of claim 20 ~~116~~ wherein the information associated with the at least two parties includes a personal key, the method further comprising:

the credential issuing entity creating the personal key, and including the personal key in the credential information.

22 ~~118.~~ The method of claim 21 ~~117~~ further comprising:

the credential issuing entity previously verifying that the personal key is unused by another party.

23 ~~119.~~ The method of claim 20 ~~116~~ further comprising:

uncoding the coded information relevant to the transaction with a joint code generated from other information associated with the at least two parties.

24 ~~120.~~ The method of claim 20 ~~116~~ wherein the information associated with the at least two parties used to generate the joint code comprises information associated with at least one present party and information associated with at least one absent party.

25 ~~121.~~ The method of claim 20 ~~116~~ wherein the information relevant to the transaction comprises coded or non-coded information.

26 20
~~122.~~ The method of claim ~~116~~ wherein the credential information further includes secret information associated with at least one of the parties only if a predetermined personal identification number (PIN), or password, or other personal information or characteristic is used by the at least one party to access the secret information.

27 20
~~123.~~ The method of claim ~~116~~ wherein the information relevant to the transaction comprises at least one information group which was previously coded to enable detection of a change in the content or structure of the information group.

28
~~124.~~ In a transaction system, a method for securing information relevant to a transaction, the transaction including at least one party, wherein a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:

creating the VAN by coding credential information with a secret key of the credential issuing entity;

authenticating the at least one of the party by using the VAN;

generating a joint code by coding first information accessed from a first one or more data storage means with second information associated with the at least one party to the transaction; and

coding the information relevant to the transaction with the joint code to generate coded information relevant to the transaction.

29 ~~125~~. The method of claim 20 ~~124~~ further comprising:

uncoding the coded information relevant to the transaction with a joint code generated from third information associated with at least one party, and fourth information accessed from a second one or more data storage means.

30 ~~126~~. The method of claim 28 ~~124~~ wherein the information relevant to the transaction comprises coded or non-coded information.

31 ~~127~~. The method of claim 28 ~~124~~ wherein the credential information further includes secret information associated with the at least one party only if a predetermined personal identification number (PIN), or password, or other personal information or characteristic is used by the at least one party to access the secret information.

32 ~~128~~. A method for coding clear information by using information associated with at least one party, wherein a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:

creating the VAN by coding credential information with a secret key of the credential issuing entity;

authenticating the at least one of the party by using the VAN;

coding a first information group with a second information group to generate a third information group, at least

one of the first and second information groups being associated with the at least one party; and

coding the clear information with the third information group to generate coded information.

33 ~~129.~~ The method of claim 32 ~~128~~ further comprising:

uncoding the coded information with a fourth information group.

34 ~~130.~~ The method of claim 32 ~~128~~ wherein the credential information further includes secret information associated with the at least one party only if a predetermined personal identification number (PIN), or password, or other personal information or characteristic is used by the at least one party to access the secret information.

35 ~~131.~~ In a multi-party transaction system, a method for securing information relevant to a transaction, the transaction including a first party and a second party, wherein a credential is previously issued to at least one of the first party and the second party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:

creating the VAN by coding credential information with a secret key of the credential issuing entity;

authenticating at least one of the first and second parties by using the VAN;

coding the information relevant to the transaction with first information associated with the first party to derive first coded information; and

coding the first coded information with first information associated with the second party to derive second coded information relevant to the transaction.

36
~~132~~. The method of claim 35 ~~131~~ further comprising:

uncoding the second coded information with second information associated with the second party to derive third coded information; and

uncoding the third coded information with second information associated with the first party to derive the information relevant to the transaction.

37
~~133~~. The method of claim 35 ~~131~~ wherein the credential information further includes secret information associated with the first party or the second party only if a predetermined personal identification number (PIN), or password, or other personal information or characteristic is used by the first party or the second party to access the secret information.

38
~~134~~. In a transaction system, a method for securing information relevant to a transaction, the transaction including at least one party, wherein a credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:

creating the VAN by coding credential information with a secret key of the credential issuing entity;

authenticating the at least one of the party by using the VAN;

coding information relevant to the transaction using information accessed from one or more data storage means to derive first coded information; and

coding the first coded information using information associated with the at least one party to the transaction to derive second coded information relevant to the transaction.

39 ~~135~~. The method of claim 38 ~~134~~ further comprising:

uncoding the second coded information using information associated with the at least one party to the transaction to derive the first coded information; and

uncoding the first coded information using information associated with information accessed from the one or more data storage means to derive the information relevant to the transaction.

40 ~~136~~. The method of claim 38 ~~134~~ wherein the credential information further includes secret information associated with the at least one party only if a predetermined personal identification number (PIN), or password, or other personal information or characteristic is used by the at least one party to access the secret information.

41 ~~137~~. A method for coding clear information by using information associated with at least one party, wherein a

credential is previously issued to the at least one party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:

creating the VAN by coding credential information with a secret key of the credential issuing entity;

authenticating the at least one of the party by using the VAN;

coding clear information with a first information group to generate a second information group, wherein the first information group is secret; and

coding the second information group with a third information group to generate a fourth information group, wherein the third information group is non-secret, at least the first or third information groups being associated with the at least one party.

42 41
~~138.~~ The method of claim ~~137~~ wherein the first or third information group includes a personal key, the method further comprising:

the credential issuing entity creating the personal key, and including the personal key in the credential information.

43 42
~~139.~~ The method of claim ~~138~~ further comprising:

the credential issuing entity previously verifying that the personal key is unused by another party.

44 41
~~140.~~ The method of claim ~~137~~ further comprising:

uncoding the fourth information group by using a fifth information group to derive the second information group; and

uncoding the second information group by using a sixth information group to recover the clear information.

45 ~~141~~. The method of claim 41 ~~137~~ wherein the credential information further includes secret information associated with the at least one party only if a predetermined personal identification number (PIN), or password, or other personal information or characteristic is used by the at least one party to access the secret information.

46 ~~142~~. In a multi-party transaction system, a method for securing information relevant to a transaction, the transaction including a first party and a second party, wherein a credential is previously issued to at least one of the first party and the second party by an entity authorized to issue a credential, the credential including a variable authentication number (VAN), the method comprising:

creating the VAN by coding credential information with a secret key of the credential issuing entity;

authenticating at least one of the first and second parties by using the VAN; and

coding the information relevant to the transaction with information associated with the first party to derive coded information relevant to the transaction, wherein the information relevant to the transaction includes information associated with the second party.

47
~~143~~. The method of claim 46 ~~142~~ wherein the information associated with the first party includes a personal key, the method further comprising:

the credential issuing entity creating the personal key, and including the personal key in the credential information.

48 47
~~144~~. The method of claim ~~143~~ further comprising:

the credential issuing entity previously verifying that the personal key is unused by another party.

49 46
~~145~~. The method of claim ~~142~~ further comprising:

uncoding the coded information relevant to the transaction with other information associated with the first party to recover the information relevant to the transaction.

50 46
~~146~~. The method of claim ~~142~~ wherein the information stored in the credential further includes secret information associated with the first party or the second party only if a predetermined personal identification number (PIN), or password, or other personal information or characteristic is used by the first party or the second party to access the secret information.

51
~~147~~. In a multi-party transaction system, a method for securing information relevant to a transaction, wherein coded information relevant to the transaction is transmitted from a first party at a first site to a second party at a second site, and a credential is previously issued to at least one of the first party and the second party by an entity authorized to issue

a credential, the credential including a variable authentication number (VAN), the method comprising:

creating the VAN by coding credential information with a secret key of the credential issuing entity;

authenticating at least one of the first and second parties by using the VAN;

the first party using first information associated with a second party to code the information relevant to the transaction to derive the coded information relevant to the transaction; and

uncoding the coded information relevant to the transaction by the second party by using second information associated with the second party to recover the information relevant to the transaction.

52 ~~148~~. The method of claim 51 ~~147~~ wherein the first or second information associated with the second party includes a personal key, the method further comprising:

the credential issuing entity creating the personal key, and including the personal key in the credential information.

53 ~~149~~. The method of claim 52 ~~148~~ further comprising:

the credential issuing entity previously verifying that the personal key is unused by another party.

54 ~~150~~. The method of claim 51 ~~147~~ wherein the information relevant to the transaction includes joint information used subsequently by the first party and the second party for coding

and uncoding information transmitted between the first and second parties.--

REMARKS

Claims 87-98, 108 and 110-150 are pending in this application. Allowed claims 87, 88, 92 and 95 were amended solely to improve their form. Allowed claim 108 was amended to improve its form and to more particularly point out and distinctly claim the invention. Allowed claims 89-91, 93-94 and 96-98 are unamended. Claims 64-66, 68-71, 73-75, 77-86, 99-107 and 109[1] were canceled and rewritten as new claims which more particularly point out and distinctly claim the invention. Additional claims were added to further define the invention.

The new claims correlate to the subject matter of the original claims as follows:

New claim	Original claim
110	64
111	New
112	New
113	65
114	66
115	101
116	68
117	New
118	New
119	69
120	70
121	71

[1] Contrary to the Office Action, there was no claim 110 prior to the current response.

New claim	Original claim
122	102
123	New
124	73
125	74
126	75
127	103
128	77
129	78
130	104
131	79
132	80
133	105
134	81
135	82
136	106
137	83
138	New
139	New
140	84
141	107
142	85
143	New
144	New
145	86
146	100
147	109
148	New
149	New
150	99

35 U.S.C. § 103(a) rejection

Claims 64-66, 68-71, 73-75, 77-86, 99-107 and 109 were rejected under 35 U.S.C. § 103(a) as being unpatentable over

Hellman. Withdrawal of this rejection as it pertains to amended claims 110-150 is respectfully requested for the reasons set forth below.

Hellman

Hellman was briefly discussed in the Response filed January 3, 1997 (entered on January 7, 1997 by the USPTO). Reference is made herein to that response for a background discussion of Hellman. The following remarks supplement the discussion in the January 3 response.

Hellman discloses a method of deriving a "common" key which is used by two parties (A and B) to encrypt and decrypt information exchanged between the parties. The common key is derived from information associated with both parties. Party A derives the common key from party A's secret key and party B's public key. Party B derives the common key from party B's secret key and party A's public key. Thus, in Hellman, the common key is derived from information associated with two parties.

Hellman's scheme lacks any disclosure whatsoever of (1) a credential or entity authorized to issue a credential, (2) a secret key associated with a credential issuing entity, and (3) a variable authentication number (VAN) or any equivalent thereto.

Assuming that the common key in Hellman is a secret key, the common key in Hellman is still not equivalent to the secret key in the amended claims. As noted above, Hellman's common key is derived from information associated with two parties to a transaction. In contrast, Applicant's secret key is

associated with a credential issuing entity, an entity which does not even exist in Hellman's scheme.

Applicant disagrees with the Examiner's statement that it would have been obvious to use a credential with Hellman, since there is no suggestion to modify Hellman to incorporate a credential in its scheme. However, assuming, *arguendo*, that it would have been obvious to use a credential with Hellman's scheme, the credential would still not have a VAN, and the VAN would not be created by coding the credential information with a secret key of the credential issuing entity, as set forth in claims 110-150.

Each of the new independent claims recite at least the following elements and steps which are nowhere disclosed or suggested by the applied references:

(1) a credential including a VAN;

(2) creating the VAN by coding credential information with a secret key of the credential issuing entity; and

(3) authenticating a party associated with a transaction by using the VAN.

Since the applied references do not disclose or suggest each and every step of the new independent claims, these claims are believed to be patentable over the applied references.

The new dependent claims are also patentable over the applied references since they incorporate all of the limitations of their respective independent claims, and because they recite additional patentable elements and steps.

Proposed Drawing Amendment

A "Proposed Drawing Amendment for Approval by Examiner" is enclosed on a separate sheet.

Conclusion

Insofar as the Examiner's rejection was fully addressed, the instant application is in condition for allowance. A Notice of Allowability of all pending claims is therefore earnestly solicited.

Respectfully submitted,

LEON STAMBLER

7/21/98 BY: Clark Jablon

(Date)

Clark A. Jablon
Registration No. 35,039
PANITCH SCHWARZE JACOBS & NADEL, P.C.
One Commerce Square
2005 Market Street, 22nd Floor
Philadelphia, PA 19103-7086
Telephone: (215) 965-1293
Facsimile: (215) 567-2991