

ZW 429592

THE UNITED STATES OF AMERICA

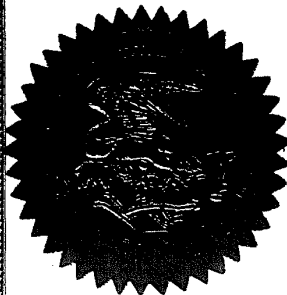
TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office


September 14, 2001

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE
RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS
OF:

APPLICATION NUMBER: 08/872,116
FILING DATE: June 10, 1997
PATENT NUMBER: 5,936,541
ISSUE DATE: August 10, 1999



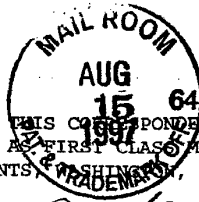
By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS


H. PHILLIPS
Certifying Officer

PART (2) OF (2) PART(S)

STAM0041461

FEDERAL RESERVE 1002



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. McLeod

DATE: August 13, 1997

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Anticipated Group Art
Leon Stambler : Unit: 2211
:
Appln. No.: 08/872,116 : Anticipated Examiner:
: B. Zimmerman
:
Filed: June 10, 1997 :
:
For: METHOD FOR SECURING :
INFORMATION RELEVANT TO A : Attorney Docket
TRANSACTION (as amended) : No. 6074-107

PRELIMINARY AMENDMENT

This preliminary amendment is being filed before receipt of a first Office Action. Please enter this preliminary amendment before examination of the application.

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

In the Claims:

Amend claim 64 as follows:

FILED
SEP 05 1997
GROUP 2200

64. (Twice Amended) In a multi-party transaction system, a method for securing information relevant to a transaction comprising the step of:

coding the information relevant to the transaction with information associated with at least one present party, and information associated with at least one absent party, [wherein the information associated with the at least one present party and the information associated with the at least one absent party are independent of each other and not derivable from each other, and at least one of the present and absent parties are pre-enrolled in the system and are preauthenticated during enrollment in the system] a credential being previously issued to at least one party, wherein information stored in the credential is non-secret, at least a portion of the non-secret information being used to authenticate the at least one party by using a variable authentication number (VAN).

Amend claim 65 as follows:

65. (Amended) The method of claim 64 wherein the coded information relevant to the transaction is uncoded with information associated with the at least one [present] absent party and with information associated with the at least one

[absent] present party to recover the relevant transaction information.

Amend claim 66 as follows:

66. (Amended) The method of claim 64 wherein the information relevant to the transaction comprises coded or non-coded information.

Cancel claim 67.

Amend claim 68 as follows:

68. (Three Times Amended) In a multi-party transaction system, a method for securing information relevant to a transaction comprising the steps of:

coding information associated with at least two parties to generate a joint code, [wherein the information associated with the at least two parties are independent of each other and not derivable from each other, at least one of the parties being pre-enrolled in the system and preauthenticated during enrollment in the system] a credential being previously issued to at least one party, wherein information stored in the credential is non-secret, at least a portion of the non-secret information being

73
(Amend)
used to authenticate the at least one party by using a variable authentication number (VAN); and

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

Amend claim 69 as follows:

69. (Amended) The method of claim 68 wherein the coded information relevant to the transaction is uncoded with [the] a joint code generated from other information associated with the at least two parties.

Amend claim 71 as follows:

71. (Amended) The method of claim 68 wherein the information relevant to the transaction comprises coded or non-coded information.

Cancel claim 72.

Amend claim 73 as follows:

73. (Three Times Amended) In a transaction system, a method for securing information relevant to a transaction comprising the steps of:

generating a joint code by coding first information accessed from a first one or more data storage means with second information associated with at least one party to the transaction, [wherein the information accessed from the one or more data storage means and the information associated with the at least one party to the transaction are independent of each other and not derivable from each other, the at least one party to the transaction being pre-enrolled in the system and preauthenticated during enrollment in the system] a credential being previously issued to at least one party, wherein information stored in the credential is non-secret, at least a portion of the non-secret information being used to authenticate the at least one party by using a variable authentication number (VAN); and

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

Amend claim 74 as follows:

74. (Amended) The method of claim 73 wherein the coded information relevant to the transaction is uncoded with [the] 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.

Amend claim 75 as follows:

75. (Amended) The method of claim 73 wherein the information relevant to the transaction comprises coded or non-coded information.

Cancel claim 76.

Amend claim 77 as follows:

77. (Three Times Amended) A method for coding clear information comprising the steps of:

coding a first information group with a second information group to generate a third information group, [wherein the first and second information groups are independent of each other and not derivable from each other and one of the first and second information groups is associated with at least one party who is preauthenticated during enrollment] at least one of the

78
(Am 4)

first and second information groups being associated with at least one party, a credential being previously issued to the at least one party, wherein information stored in the credential is non-secret, at least a portion of the non-secret information being used to authenticate the at least one party by using a variable authentication number (VAN); and

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

Amend claim 78 as follows:

79

78. (Amended) The method of claim 77 wherein the coded information [can be] is uncoded with [the third] a fourth information group.

Amend claim 79 as follows:

710

79. (Twice Amended) In a multi-party transaction system, a method for securing information relevant to a transaction comprising the steps of:

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

coding the first coded information with information associated with a second party to derive second coded information, [wherein the information associated with the first party and the second party is independent of each other and not derivable from each other, at least one of the first party and the second party being pre-enrolled in the system and preauthenticated during enrollment in the system] a credential being previously issued to at least one party, wherein information stored in the credential is non-secret, at least a portion of the non-secret information being used to authenticate the at least one party by using a variable authentication number (VAN).

Amend claim 81 as follows:

81. (Twice Amended) In a transaction system, a method for securing information relevant to a transaction comprising the steps of:

coding the information relevant to a transaction with information accessed from one or more data storage means to derive first coded information, and

coding the first coded information with information associated with at least one party to the transaction to derive

second coded information, [wherein the information accessed from the one or more data storage means and the information associated with the at least one party to the transaction are independent of each other and not derivable from each other, the at least one party to the transaction being pre-enrolled in the system and preauthenticated during enrollment in the system] a credential being previously issued to at least one party, wherein information stored in the credential is non-secret, at least a portion of the non-secret information being used to authenticate the at least one party by using a variable authentication number (VAN).

Amend claim 83 as follows:

83. (Twice Amended) A method for coding clear information comprising the steps of:

- coding the 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, [and the first and third information groups are independent of each other and not

7/12
(Am. 4)

derivable from each other and one of the first and third
information groups is associated with a party who is
preauthenticated during enrollment] at least the first or third
information groups being associated with at least one party, a
credential being previously issued to the at least one party,
wherein information stored in the credential is non-secret, at
least a portion of the non-secret information being used to
authenticate the at least one party by using a variable
authentication number (VAN).

Amend claim 84 as follows:

84. (Amended) The method of claim 83 [wherein the]
further comprising the step of recovering the clear information
[is recovered comprising] by performing the steps of:
uncoding the fourth information group by using [the
third] a fifth information group to derive the second information
group; and
uncoding the second information group by using [the
first] a sixth information group to recover the clear
information.

Amend claim 85 as follows:

85. (Three Times Amended) In a multi-party transaction system, a method for securing information relevant to a transaction comprising the step of:

coding the information relevant to a transaction with information associated with a first party to derive coded information relevant to the transaction, wherein the information relevant to the transaction includes information associated with a second party, [the information associated with the first party and the information associated with the second party being independent of each other and not derivable from each other, at least one of the first and second parties being pre-enrolled in the system and being preauthenticated during enrollment in the system] a credential being previously issued to the second party, wherein information stored in the credential is non-secret, at least a portion of the non-secret information being used to authenticate the second party by using a variable authentication number (VAN).

Add new claims 99-109 as follows:

--99. The method of claim 109 wherein the information relevant to the transaction includes joint information used subsequently by the first party and the second party for coding

-11-

STAM0041472

and uncoding information transmitted between the first and second parties.

100. The method of claim 85 wherein the information stored in the credential further includes secret information associated with the second party only if a predetermined personal identification number (PIN), or password, or other personal information or characteristic is used by the second party to access the secret information.

101. The method of claim 64 wherein the information stored in the credential 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.

102. The method of claim 68 wherein the information stored in the credential 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.

103. The method of claim 73 wherein the information stored in the credential 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.

104. The method of claim 77 wherein the information stored in the credential 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.

105. The method of claim 79 wherein the information stored in the credential 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.

106. The method of claim 81 wherein the information stored in the credential 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.

107. The method of claim 83 wherein the information stored in the credential 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.

108. 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 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 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 the recovered EDC1 and EDC5 to generate a seventh error detection code (EDC7);

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

109. 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, the method comprising the step of:

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, the coded information relevant to the transaction being subsequently uncoded by the second party by using second information associated with the second party to recover the information relevant to the transaction, a credential being previously issued to the second party, wherein information stored in the credential is non-secret, at least a portion of the non-secret information being used by the first party to authenticate the second party by using a variable authentication number (VAN).--

REMARKS

Claims 64-66, 68-71, 73-75 and 77-109 are pending in this application. Claims 64-66, 68, 69, 71, 73-75, 77-79, 81 and 83-85 were amended to more particularly point out and distinctly claim the invention. Claims 67, 72 and 76 were canceled and their subject matter was incorporated into respective claims 66, 71 and 75. New claims 99-109 were added to further define the invention.

The following comments are provided to assist the Examiner in evaluating the patentability of the present set of claims over the previously applied reference in the parent application (Maurer).

Independent claims 64, 68, 73, 77, 79, 81, 83, 85 and 109 recite the use of a credential having non-secret information stored thereon, and the use of a VAN for authentication. A credential may be a check, document, record, electronic storage medium, or the like. Reference is made to the specification for a more comprehensive explanation of credentials and VANs.

Maurer relates to a method of generating a cipher key. Nowhere does Maurer disclose or suggest the use of a credential as set forth in claims 64, 68, 73, 77, 79, 81, 83, 85 and 109.

Independent claims 87 and 92 were previously discussed in the parent application and were allowed over Maurer. See page 9 of the Amendment After Final dated September 19, 1997 (filed in the USPTO on September 23, 1996). The remarks on page 9 are incorporated herein in their entirety. Accordingly, these claims are unamended in the present application.

The combination of steps in new claim 108 are nowhere disclosed or suggested by Maurer.

Prompt examination and allowance of the present application is requested.

Respectfully submitted,

LEON STAMBLER

8/13/97

(Date)

BY:

Clark A. Jablon

Clark A. Jablon

Registration No. 35,039

PANITCH SCHWARZE JACOBS & NADEL, P.C.

1601 Market Street, 36th Floor

Philadelphia, PA 19103

Telephone: (215) 567-2020

Facsimile: (215) 567-2991

CAJ:LLK:eam



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. McLeod

DATE: August 13, 1997

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re.:	Patent application of	:
	Leon Stambler	: Anticipated Group Art Unit:
		: 2211
Appln. No.:	08/872,116	:
		: Anticipated Examiner:
Filed:	June 10, 1997	: B. Zimmerman
		:
		: Attorney Docket
For:	METHOD FOR SECURING	: No. 6074-1U7
	INFORMATION RELEVANT TO A	:
	TRANSACTION (as amended)	:

RECEIVED
SEP 05 1997
GROUP 2200

AMENDMENT COVER SHEET

Transmitted herewith is an Amendment in the above identified application.

☒ A verified statement to establish small entity status under 37 CFR 1.9 and 1.27 is

☒ already on file;

☐ enclosed.

☐ No additional fee is required.

☐ An Information Disclosure Statement with one copy of each of the cited patents is also attached.

The fee has been calculated as shown below:

STAM0041481

					SMALL ENTITY		LARGE ENTITY	
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NO. PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDIT FEE	RATE	ADDIT. FEE
TOTAL	43	(-)	or 20	= 8	X11	\$ 88	X22	\$
INDEP.	12	(-)	or 3	= 2	X40	\$ 80	X80	\$
1ST PRESENTATION OF MULTIPLE DEPENDENT CLAIMS					+ \$130	\$	+\$260	\$
					TOTAL	\$168	TOTAL	\$

☐ The applicant(s) hereby petition(s) for any extension of time which may be required in connection with the filing of the enclosed paper(s). (Petition and Fee for _____ month(s) extension is enclosed.)

☒ The Assistant Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 16-0235. One additional copy of this sheet is attached for accounting purposes.

☒ The above calculated additional claim fees \$168.00.

☒ Any additional fees under 37 CFR 1.16 or 1.17.

Respectfully submitted,

LEON STAMBLER

August 13, 1997
(Date)

By:

Clark Jablon

CLARK A. JABLON

Registration No. 35,039

PANITCH SCHWARZE JACOBS & NADEL, P.C.

1601 Market Street - 36th Floor

Philadelphia, PA 19103-2398

Telephone: (215) 567-2020

Facsimile: (215) 567-2991

CAJ:eam
Enclosures

PSJN2/115658.1

-2-

STAM0041482

04/16/98 14:31

215 567 2991

PANITCH

001/018

OFFICIAL

OFFICIAL

FAX RECEIVED

APR 16 1998

GROUP 2600

PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS

One Commerce Square - 2005 Market Street - 22nd Floor - Philadelphia, PA 19103-7086
TELEPHONE: (215) 567-2020 - FACSIMILE: (215) 567-2991 - E-MAIL: psjn@psjn.com

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that this paper is being facsimile transmitted
to the U.S. Patent and Trademark Office on the date shown below

Elizabeth A. McCloud

Type or print name of person signing certification

Elizabeth A. McCloud April 16, 1998
Signature Date

FACSIMILE COVER SHEET

Examiner: B. Zimmerman

FAX No.: 703-305-3988

Group Art Unit: 2735

Date: April 16, 1998

From: Clark A. Jablon

FAX Operator: Elizabeth A. McCloud

Re: U.S. Patent Application No. 08/872,116 For "METHOD FOR SECURING
INFORMATION RELEVANT TO A TRANSACTION"

Title of Paper sent via Facsimile: (1) Communication; (2) previously filed Third Supplemental
Information Disclosure Statement, (3) previously filed PTO-1449's, (4) previously filed "Notice
of Change of Address" and (5) Postcard receipt bearing the PTO mailroom stamp of December
29, 1997 for items (2), (3) and (4).

Time: 2:35

PSJ&N File No: 6074-1U7

Page 1 of 10 pages

IF YOU DO NOT RECEIVE ALL THE PAGES, PLEASE CONTACT
Elizabeth A. McCloud AT 215-965-1295

See attachments referred to above.

**THIS FACSIMILE MESSAGE IS CONFIDENTIAL AND MAY CONTAIN ATTORNEY PRIVILEGED
INFORMATION INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR COMPANY NAMED ABOVE.**

If you are not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, any dissemination, distribution or copying of this
communication is strictly prohibited. If you have received this communication in error, please immediately call us so that we may arrange for the return of the
original message to us. Thank you!

04/16/88

14:32

21 215 567 2981

PANITCH

002/010

OFFICIAL

FAX RECEIVED

APR 16 1998

GROUP 2600

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2735
Leon Stambler :
:
Appln. No.: 08/872,116 : Examiner: B. Zimmerman
:
Filed: June 10, 1997 :
:
For: METHOD FOR SECURING :
INFORMATION RELEVANT TO A : Attorney Docket
TRANSACTION : No. 6074-1U7

COMMUNICATION

This communication is being submitted to facilitate three outstanding issues in the above-identified matter. On April 15, 1998, Applicant's undersigned representative telephoned the Examiner about the issues and the Examiner suggested that this correspondence be filed to more quickly resolve the outstanding issues.

The outstanding issues are as follows:

(1) A Third Supplemental Information Disclosure Statement (IDS) was filed on December 23, 1997 and was apparently not yet matched up with the application file when the Examiner issued the Office Action dated April 8, 1998. Applicant requests that the Third Supplemental IDS be formally considered and that a signed copy of the PTO-1449s be provided to the Applicant.

Enclosed herewith are the following items related to the Third Supplemental IDS:

PSJNZ/161119.1

-1-

(a) Copy of Third Supplemental IDS and PTO-1449s as filed. Due to the large number of cited references, additional copies are not enclosed. Copies will be provided upon request if the PTO cannot locate the originally filed papers. To assist the Examiner in locating copies of these references, similar IDSs were filed in corresponding Application Nos. 08/747,174 and 08/855,561.

(b) Postcard receipt for such papers bearing a PTO mailroom stamp of December 29, 1997.

(2) A Notice of Change of Address was submitted in the present application, but was apparently not matched up with the application file when the Examiner issued the Office Action dated April 8, 1998. Applicant requests that the change of address be processed before any additional correspondence is mailed by the PTO.

Enclosed herewith are the following items related to the change of address:

(a) Copy of Notice of Change of Address, as filed.

(b) Postcard receipt for this paper bearing a PTO mailroom stamp of May 22, 1997 (see same postcard receipt as in issue (1)).

(3) The claims listed as pending and rejected in the Office Action dated April 8, 1998 do not conform with the currently pending claims. The pending claims are claims 64-66, 68-71, 73-75 and 77-109, as summarized on page 18, paragraph 1 of the Preliminary Amendment filed August 13, 1997. The Examiner

agreed to reissue the Office Action setting forth the corrected claim status.

Please telephone Applicant's undersigned attorney if additional information or materials are needed to resolve any of the outstanding issues.

Respectfully submitted,

LEON STAMBLER

4/16/98
(Date)

BY:

Clark A. Jablon

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

CAJ:eam

04/16/98

14:32

1 215 567 2991

PANITCH

005/010

OFFICIAL

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. McLeod

DATE:

12/23/97

PATENT

FAX RECEIVED**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re: Patent Application of
Leon Stambler

: Group Art Unit 2211

APR 16 1998

Appln. No.: 08/872,116

: Examiner: B. Zimmerman

GROUP 2600

Filed: June 10, 1997

For: METHOD FOR SECURING
INFORMATION RELEVANT TO A
TRANSACTION (as amended)

: Attorney Docket
: No. 6074-1U7

THIRD SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

This Second Supplemental Information Disclosure Statement (IDS) is being filed before the first Office Action on the merits. Accordingly, no fee or certification is believed to be due for consideration of the cited references.

It is requested that the enclosed references listed on the attached Second Supplemental IDS Form PTO-1449 be considered by the Patent Examiner in connection with the above-identified application and be made of record therein.

These references are being made of record because Applicant recently became aware of U.S. Patent No. 5,677,955 (Doggett et al.) and the references cited therein. With respect to the publications cited in the patent, only the publications having publication dates before the effective filing date of the present application (which is November 17, 1992) are cited. Furthermore, Applicant was not able to obtain copies of two of the articles cited in the publication section which predate the effective filing date of the present application, namely, the articles entitled "Industry Players Discuss...Dec. 20, 1990" and "New, Practical ACH...Apr. 26, 1990." Nor is Applicant aware of the contents of such articles. Accordingly, neither of these articles are cited either.

PSJN2/13932Z,1

- 1 -

STAM0041487

04/18/98 14:33

215 567-2991

PANITCH

006/010

Independent consideration and acknowledgment of the enclosed references are respectfully requested.

Respectfully submitted,

LEON STAMBLER

12/23/97

(Date)

By:

Clark A. Jablon

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) 965-1923

Facsimile: (215) 567-2991

E-Mail: psjn@psjn.com

CAJ:eam
Enclosure

04/18/98

14:33

☎ 215 567 2991

PANITCH

007/010

Sheet 1 of 2

Form PTO-1449 (REV. 8-83)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY DOCKET NO.: 6074-1U7		APPLICATION NO.: 08/872,116	
THIRD SUPPLEMENTAL INFORMATION DISCLOSURE CITATION (Form PTO-1449 Modified 5/95) (Use several sheets if necessary)				APPLICANT: Leon Stambler			
				FILING DATE: June 10, 1997		GROUP ART UNIT: 2241 2735	
U.S. PATENT DOCUMENTS							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE IF APPROPRIATE
b2		4,264,808	04/1981	Owens <i>et al.</i>			
		4,423,287	12/1983	Zeidler			
		4,823,264	04/1989	Deming			
		5,187,351	02/1993	Clary			
		5,191,613	03/1993	Graziano <i>et al.</i>			
		5,218,637	06/1993	Angebaud <i>et al.</i>			
		5,224,162	06/1993	Okamoto <i>et al.</i>			
		5,283,829	02/1994	Anderson			
		5,297,202	03/1994	Kapp <i>et al.</i>			
		5,321,751	06/1994	Ray <i>et al.</i>			
		5,326,959	07/1994	Pcrazza			
		5,453,601	09/1995	Rosen			
		5,455,407	10/1995	Rosen			
		5,465,299	11/1995	Matsumoto <i>et al.</i>			
		5,473,690	12/1995	Grimonprez <i>et al.</i>			
b2		5,530,755	06/1996	Pailles <i>et al.</i>			
FOREIGN PATENT DOCUMENTS							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION YES NO
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)							
b2		Shipley C., "I threw away my checkbook", PC-Computing, vol. 3, No. 11, pp. 112, 114-115, 118-120, Nov. 1990.					
b2		Diamond S., "Check Processing Takes a New Turn", Computers in Banking, vol. 5, No. 3, pp. 50-55, March 1988.					
EXAMINER <i>B. J. ...</i>				DATE CONSIDERED 4/18/98			
*EXAMINER: Initial if citation 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.							

PS/NZ/137596.1

STAM0041489

04/18/98

14:33

215 587 2991

PANITCH

008/010

Sheet 2 of 2

Form PTO-1449 (REV. 2-83)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY DOCKET NO.: 6074-1U7		APPLICATION NO.: 08/872,116	
THIRD SUPPLEMENTAL INFORMATION DISCLOSURE CITATION (Form PTO-1449 Modified 5/95) (Use several sheets if necessary)				APPLICANT: Leon Stambler		GROUP ART UNIT: 441 2735	
				FILING DATE: June 10, 1997			
U.S. PATENT DOCUMENTS							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE IF APPROPRIATE
80		5,677,955	10/1997	Doggett <i>et al.</i>			
FOREIGN PATENT DOCUMENTS							
EX. INIT	DOCU- MENT	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION YES NO
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)							
80		Iida J., "Electronic Presentment Due for N.Y. Test", American Banker, vol. 157, No. 143, p. 3, July 27, 1992.					
		Torrez A., "Banking Industry Looks at Changing Check Guarantees", The Business Journal-Phoenix & The Valley of the Sun, vol. 9, No. 29, pp. 13-14, May 29, 1989.					
		Sullivan D., "Bank Technology Trick or Treat?", Bankers Monthly, vol. 109, No. 11, pp. 10, 12-14, 18, 20, November 1992.					
		Scidenberg, "Bell Companies Now Testing Smart Card Offering Increased Feature Functionality", Card News, vol. 5, No. 10, pp. 5-6, May 21, 1990.					
		"General Magnaplate Corporation Issues Three-Month Report to Stockholders", PR Newswire, 1 page, November 11, 1992.					
		Byles T., "More Companies Are Paying Bills Electronically", Journal of Commerce, p. 2B, May 5, 1988.					
80		Carreker J.D., "Strides in Electronic Checking Transforming Payment System", vol. 68, No. 3, pp. 18-19, 22, 24, 26, 28, 30, March 1992.					
EXAMINER				DATE CONSIDERED			
BZ <i>manman</i>				4/18/98			
*EXAMINER: Initial if citation 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.							

04/16/88

14:33

☎ 215 567 2991

PANITCH

009/010

OFFICIAL

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 OF PATENTS, WASHINGTON, DC 20231, ON THE DATE INDICATED BELOW.

BY: Elizabeth R. McLeod DATE: 12/23/97

**PATENT
FAX RECEIVED**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE APR 16 1998

In re:	Patent Application of Leon Stambler	: Group Art Unit 2211	GROUP 2600
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. 6074-1U7	

NOTICE OF CHANGE OF ADDRESS

Please change the correspondence address of the attorneys of record in the above-identified patent application as follows:

**Panitch Schwarze Jacobs & Nadel, P.C.
One Commerce Square
2005 Market Street - 22nd Floor
Philadelphia, PA 19103-7086**

The corresponding attorney and the telephone number are as indicated below.

Respectfully submitted,

December 23, 1997
(Date)

By: Clark Jablon
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
E-Mail: psjn@psjn.com

CAJ:eam

STAM0041491

04/16/98 14:34

215 567 2981

PANITCH

010/010

FAX RECEIVED

APR 16 1998

GROUP 2600

CAI/eam

ATTORNEY DOCKET # 6074-1117 TODAY'S MAILING DATE 12/23/97

PAY/INSTR. / REG/OPP/CANC./# 08/872,116

CERT. of MAIL CERT. of SERV/EXPRESS MAIL

OF: Loan Standards

FOR: Method for securing information

RECEIPT IS ACKNOWLEDGED FOR THE FOLLOWING:

TRADEMARK APPLICATION

Specimens

RENEWAL/AFF 8/AFF 8 & 15

PAT APP (NEW/DIV/CP/FWC/RE)

Dec & Power of Atty

Pages Specifications

Preliminary Amendment

Claims

Sheets Drawings

Type

COVER SHEET/LETTER/ORDER

AMENDMENT/REQ. RECONS

ASSIGN/CHG NAME/MERGER/SEC. INT.

VER STMT/SMALL ENTITY

NOTICE OF APPEAL/BRIEF COPIES

FINAL FEE

INFORM. DECL

INF. DISCL. STATEMENT PT 1/4/97 1 ref.

PRIORITY DOC.

PET/MOT. FOR EXT. TIME

Fee authorization charge Deposit Acct. #16-0235 \$

OTHER (PAPER TITLE) Change of Address

STAM0041492

PTO-103X
(Rev. 8-95)

FILING RECEIPT



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTORNEY DOCKET NO.	DRWGS	TOT CL	IND CL
08/872,116	06/10/97	2211	\$830.00	6074-1U7	15	35	10

CLARK A JABLON
PANITCH SCHWARZE JACOBS & NADEL
1601 MARKET STREET
36TH FLOOR
PHILADELPHIA PA 19103-2398

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please write to the Application Processing Division's Customer Correction Branch within 10 days of receipt. Please provide a copy of the Filing Receipt with the changes noted thereon.

Applicant(s)

LEON STAMBLER, PARKLAND, FL.

CONTINUING DATA AS CLAIMED BY APPLICANT-

THIS APPLN IS A CON OF 08/446,369 05/22/95
WHICH IS A DIV OF 08/122,071 09/14/93 PAT 5,524,073
WHICH IS A DIV OF 07/977,385 11/17/92 PAT 5,267,314

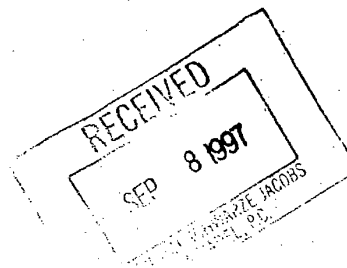
FOREIGN FILING LICENSE GRANTED 08/08/97

TITLE

METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION

PRELIMINARY CLASS: 340

RECEIVED
NOV 10 1997
GROUP 2200



(see reverse)

MDC

STAM0041493

**LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15**

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "FOREIGN FILING LICENSE GRANTED" followed by a date appears on the reverse side of this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.11. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related application(s) filed under 37 CFR 1.62 which meets the provisions of 37 CFR 5.15(a). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations, especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR Parts 121-128)); the Office of Export Administration, Department of Commerce (15 CFR 370.10 (j)); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "FOREIGN FILING LICENSE GRANTED" DOES NOT appear on the reverse side of this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

STAM0041494



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, DC 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
087872.116	06/10/97	STAMBLER	6074-107

LM32/0408

CLARK A JABLON
PANITCH SCHWARZE JACOBS & NADEL
1601 MARKET STREET
36TH FLOOR
PHILADELPHIA PA 19103-2398

EXAMINER
ZIMMERMAN, B

ART UNIT 2735	PAPER NUMBER 24
------------------	--------------------

DATE MAILED: 04/08/98

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

Commissioner of Patents and Trademarks

STAM0041495

Office Action Summary	Application No. 08/872,116	Applicant(s) Stambler	
	Examiner Brian Zimmerman	Group Art Unit 2735	

☒ Responsive to communication(s) filed on Aug 15, 1997.

☐ This action is **FINAL**.

☐ 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.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) 64-110 is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☒ Claim(s) 87-98 and 108 is/are allowed.

☒ Claim(s) 64-86, 99-107, 109, and 110 is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

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

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☐ Notice of References Cited, PTO-892

☒ Information Disclosure Statement(s), PTO-1449, Paper No(s). 22

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

— SEE OFFICE ACTION ON THE FOLLOWING PAGES —

EXAMINER'S RESPONSE

Status of Application.

1. In response to the applicant's amendment received on 8/15/97. The examiner has considered the new presentation of claims and applicant arguments in view of the disclosure and the present state of the prior art. And it is the examiner's position that claims 64-86,99-107,109,110 are unpatentable for the reasons set forth in this office action:

CLAIMS

2. Claim 87-98,108 are allowable over the prior art of record.

ART REJECTION

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

15

4. Claim 64-86,99-107,109,110 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman and the admitted prior art.

Hellman clearly shows the multi-party secure transaction system which is claimed. See the abstract, figure 1, and col. 2 lines 53+. It is verily well known to send coded information or noncoded information (digital or analog) between stations in an encrypted manner, and by claiming both, the applicant has effectively shown that this

20



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
07/15/97	07/15/97	STAMBLER	L 6074-1U7

CLARK A JABLON
PATRICIA SCHWARZE JACOBS & NADEL
ONE COMMERCE SQUARE
2005 MARKET STREET-22ND FLOOR
PHILADELPHIA PA 19103-7086

LM32/0422

EXAMINER
ZIMMERMAN, B

ART UNIT	PAPER NUMBER
2735	25

DATE MAILED: 04/22/98

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

Commissioner of Patents and Trademarks

08/872116
2735

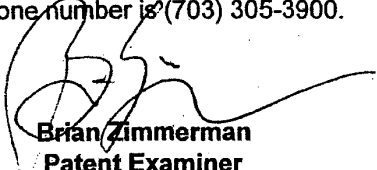
3

In the present application, the applicant admits that special authentication procedures have been utilized to assure the authenticity of documents or credentials. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have send secret and non secret information from a credential utilizing the Hellman's authentication procedures since this security exchange method would assure the authenticity of the credentials.

CONTACT INFORMATION

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian Zimmerman whose telephone number is (703) 305-4796.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.


Brian Zimmerman
Patent Examiner
Art Unit 2735

703-305-4796
April 06, 1998

Office Action Summary	Application No. 08/872,116	Applicant(s) Stambler
	Examiner Brian Zimmerman	Group Art Unit 2735

☒ Responsive to communication(s) filed on 8/15/97 and 4/16/98

☐ This action is **FINAL**.

☐ 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.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) 64-66, 68-71, 73-75, and 77-110 is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☒ Claim(s) 87-98 and 108 is/are allowed.

☒ Claim(s) 64-66, 68-71, 73-75, 77-86, 99-107, 109, and 110 is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

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

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

— SEE OFFICE ACTION ON THE FOLLOWING PAGES —

EXAMINER'S RESPONSE

Status of Application.

1. In response to the applicant's amendment received on 8/15/97. The examiner has considered the new presentation of claims and applicant arguments in view of the disclosure and the present state of the prior art. And it is the examiner's position that claims 64-86,99-107,109,110 are unpatentable for the reasons set forth in this office action:

CLAIMS

2. Claim 87-98,108 are allowable over the prior art of record.

ART REJECTION

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

15

4. Claim 64-66,68-71,73-75,77-86,99-107,109,110 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman and the admitted prior art.

Hellman clearly shows the multi-party secure transaction system which is claimed. See the abstract, figure 1, and col. 2 lines 53+. It is verily well known to send coded information or noncoded information (digital or analog) between stations in an encrypted manner, and by claiming both, the applicant has effectively shown that this

20

08/872116
2735

3

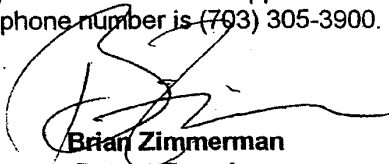
is not essential to the operation of the claimed device.

In the present application, the applicant admits that special authentication procedures have been utilized to assure the authenticity of documents or credentials. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have send secret and non secret information from a credential utilizing the Hellman's authentication procedures since this security exchange method would assure the authenticity of the credentials.

CONTACT INFORMATION

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian Zimmerman whose telephone number is (703) 305-4796.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.


Brian Zimmerman
Patent Examiner
Art Unit 2735

703-305-4796
April 17, 1998

STAM0041502

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. McLeod

DATE: 7/21/98



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2735
Leon Stambler :
Appln. No.: 08/872,116 : Examiner: B. Zimmerman
Filed: June 10, 1997 :
For: METHOD FOR SECURING :
INFORMATION RELEVANT TO A : Attorney Docket
TRANSACTION (as amended) : No. 6074-1U7

RECEIVED
98 JUL 29 PM 2:59
GROUP 2100

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:

PSJNZ/172870.1

-1-

G

07/27/1998 RTSGRYE 00000069 160235
01 FC:203 110.00 CH

STAM0041503

109

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

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:

2 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

Amend 92
uncoding the coded information using the derived second coded authentication information to recover the clear information.

Amend claim 92 as follows:

92 92. (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] using 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:

93 95. (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

103
103 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 [transaction] 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
~~111~~. The method of claim ¹⁴~~110~~ wherein the information associated with the present party or the absent party includes a 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
~~112~~. The method of claim ¹⁵~~111~~ further comprising:
the credential issuing entity previously verifying that the personal key is unused by another party.

¹⁷
~~113~~. The method of claim ¹⁴~~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
~~114~~. The method of claim ¹⁴~~110~~ wherein the information relevant to the transaction comprises coded or non-coded information.

¹⁹
~~115~~. The method of claim ¹⁴~~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, 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
~~122.~~ The method of claim ²⁰~~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
~~123.~~ The method of claim ²⁰~~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
~~138~~: The method of claim ⁴¹~~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
~~139~~: The method of claim ⁴²~~138~~ further comprising:
the credential issuing entity previously verifying that the personal key is unused by another party.

⁴⁴
~~140~~: The method of claim ⁴¹~~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* 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
~~144~~. The method of claim ⁴⁷~~143~~ further comprising:

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

⁴⁹
~~145~~. The method of claim ⁴⁶~~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
~~146~~. The method of claim ⁴⁶~~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

Handwritten initials/signature

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 109¹ 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:

<u>New claim</u>	<u>Original claim</u>
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.

<u>New claim</u>	<u>Original claim</u>
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

(Date)

BY:

Clark Jablon

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

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. McLeod

DATE: 7/21/98



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2735
Leon Stambler :
:
:
Appln. No.: 08/872,116 : Examiner: B. Zimmerman
:
:
Filed: June 10, 1997 :
:
For: METHOD FOR SECURING :
INFORMATION RELEVANT TO A : Attorney Docket
TRANSACTION (as amended) : No. 6074-1U7

SUBMISSION OF PROPOSED DRAWING AMENDMENT
FOR APPROVAL BY EXAMINER (37 CFR 1.123)

Attached please find a copy of the original informal sheets of drawings with red ink markings, showing the proposed changes to the drawings in this application, for which the approval of the Examiner is requested. The proposed drawing changes are as follows:

1. Fig. 9: Change "REMOTE PIN" to --REMOTE COMPUTER--.
2. Fig. 10B: Add a label "132" to the coder block.

A detailed explanation of the corrections is provided immediately below:

PSJN2/178352.1

-1-

1. Correction to Fig. 9: The reference to a "Remote PIN" should have read "Remote Computer" to be consistent with page 17, lines 1-6 of the specification.

2. Correction to Fig. 10B: The coder should be labeled as block "132" to be consistent with page 21, lines 27-33 of the specification.

The above-identified corrections are fully supported by the original specification and thus do not constitute new matter. Correction is thus believed to be permitted.

Respectfully submitted,

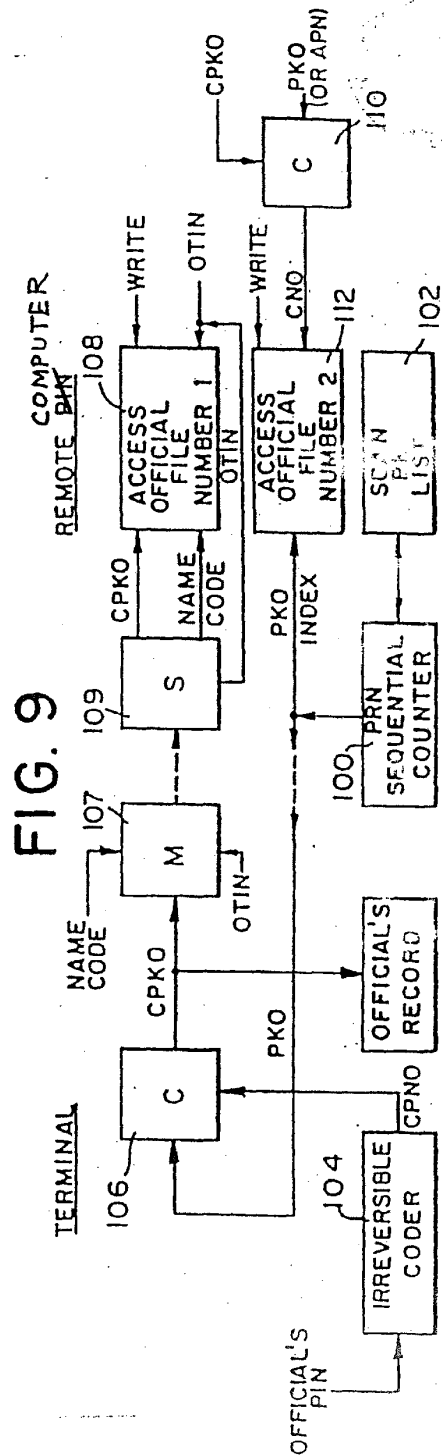
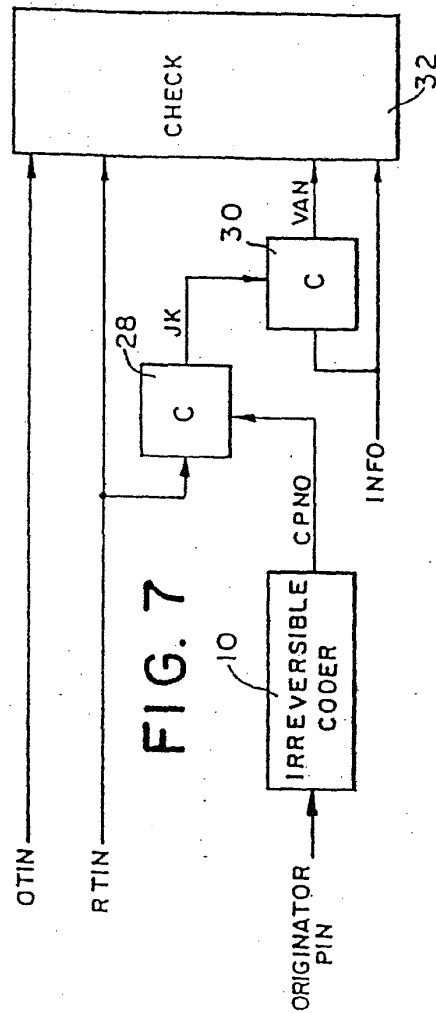
LEON STAMBLER

7/21/98
(Date)

BY:

Clark A. Jablon

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





PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

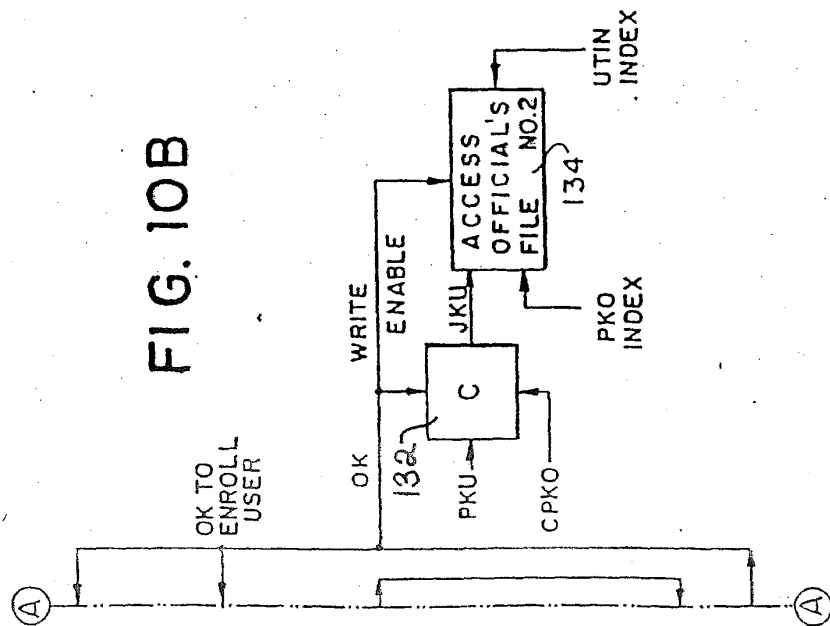
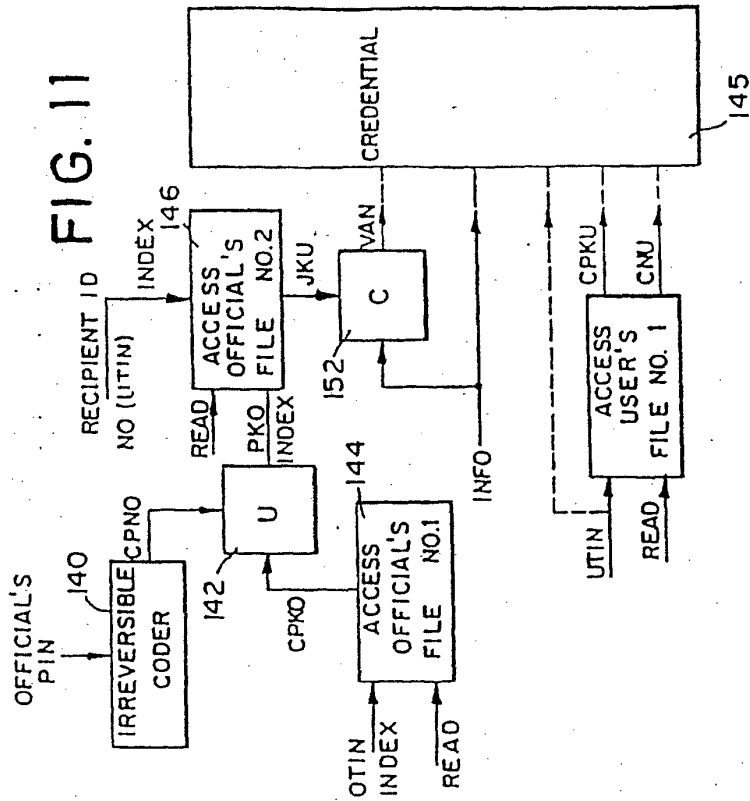
TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

Attachment to "Submission of Proposed Drawing Amendment for Approval by
Examiner"

ATTORNEY DOCKET NO.: 6074-1U7

RECEIVED
98 JUL 23 PM 2:59
GROUP 2753

STAM0041528



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

PPPLICANT: Leon Stambler

PPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

Attachment to "Submission of Proposed Drawing Amendment for Approval by
Examiner"

ATTORNEY DOCKET NO.: 6074-1U7

STAM0041530

GAU 2735/\$

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. McLeod

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	:
		: Attorney Docket
For:	METHOD FOR SECURING	: No. 6074-1U7
	INFORMATION RELEVANT TO A	:
	TRANSACTION (as amended)	:

AMENDMENT COVER SHEET

Transmitted herewith is an Amendment in the above identified application.

- ☒ [X] A verified statement to establish small entity status under 37 CFR 1.9 and 1.27 is
- ☒ [X] already on file;
- ☐ [] enclosed.
- ☐ [] No additional fee is required.
- ☐ [] An Information Disclosure Statement with one copy of each of the cited patents is also attached.

The fee has been calculated as shown below:

STAM0041531

					SMALL ENTITY		LARGE ENTITY	
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NO. PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDIT FEE	RATE	ADDIT. FEE
TOTAL	53	(-)	43	= 10	X11	\$110	X22	\$
INDEP.	12	(-)	12	= 0	X41	\$	X82	\$
1ST PRESENTATION OF MULTIPLE DEPENDENT CLAIMS					+\$135	\$	+\$270	\$
					TOTAL	\$110	TOTAL	\$

☒ The applicant(s) hereby petition(s) for any extension of time which may be required in connection with the filing of the enclosed paper(s). (Petition and Fee for _____ month(s) extension is enclosed.)

☒ The Assistant Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 16-0235. One additional copy of this sheet is attached for accounting purposes.

☒ The above calculated additional claim fees of \$110.00.

☒ Any additional fees under 37 CFR 1.16 or 1.17.

Respectfully submitted,

LEON STAMBLER

July 21, 1998
(Date)

By:

Clark Jablon

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) 567-2020

Facsimile: (215) 567-2991

E-Mail: psjn@psjn.com

CAJ:eam
Enclosures

PSJN2/178421.1

-2-

STAM0041532



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

2735

CHANGE OF ADDRESS/POWER OF ATTORNEY

LOCATION 27C1 SERIAL NUMBER 08872116 PATENT NUMBER

THE CORRESPONDENCE ADDRESS HAS BEEN CHANGED TO CUSTOMER #

THE PRACTITIONERS OF RECORD HAVE BEEN CHANGED TO CUSTOMER #

THE FEE ADDRESS HAS BEEN CHANGED TO CUSTOMER # 570

ON 07/10/98 THE ADDRESS OF RECORD FOR CUSTOMER NUMBER 570 IS:

PANITCH SCHWARZE JACOBS & NADEL
ONE COMMERCE SQUARE
2005 MARKET STREET 22ND FLOOR
PHILADELPHIA PA 19103

AND THE PRACTITIONERS OF RECORD FOR CUSTOMER NUMBER 570 ARE:

22130	22825	25918	27363	27633	28959	28959	29546	32886	34626
35039	35039	35837	36317	36317	40961	40961	40961		

PTO INSTRUCTIONS: PLEASE TAKE THE FOLLOWING ACTION WHEN THE
CORRESPONDENCE ADDRESS HAS BEEN CHANGED TO CUSTOMER NUMBER:
RECORD, ON THE NEXT AVAILABLE CONTENTS LINE OF THE FILE JACKET,
'ADDRESS CHANGE TO CUSTOMER NUMBER'. LINE THROUGH THE OLD
ADDRESS ON THE FILE JACKET LABEL AND ENTER ONLY THE 'CUSTOMER
NUMBER' AS THE NEW ADDRESS. FILE THIS LETTER IN THE FILE JACKET.
WHEN ABOVE CHANGES ARE ONLY TO FEE ADDRESS AND/OR PRACTITIONERS
OF RECORD, FILE LETTER IN THE FILE JACKET.

PTO-FMD
TALBOT-1/97



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, DC 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
06/872,116	06/10/97	STAMBLER	0074-107

000570 LM32/0915

PANITCH SCHWARZE JACOBS & NADEL

ONE COMMERCE SQUARE

2005 MARKET STREET 22ND FLOOR

PHILADELPHIA PA 19103

EXAMINER
ZIMMERMAN, D

ART. UNIT PAPER NUMBER
2705 28

DATE MAILED:

09/15/98

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

Commissioner of Patents and Trademarks

Office Action Summary	Application No. 08/872,116	Applicant(s) Stambler
	Examiner Brian Zimmerman	Group Art Unit 2735

☒ Responsive to communication(s) filed on Jul 23, 1998

☐ This action is **FINAL**.

☐ 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.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) 87-98, 108, and 110-150 is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) 87-98, 108, and 110-150 is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☒ The proposed drawing correction, filed on 7/23/98 is ☒ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

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

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

— SEE OFFICE ACTION ON THE FOLLOWING PAGES —

08/872116
2735

2

EXAMINER'S RESPONSE

Status of Application.

1. In response to the applicant's amendment received on 7/30/98. The examiner has considered the new presentation of claims and applicant arguments in view of the disclosure and the present state of the prior art. And it is the examiner's position that claims 87-98,108,110-150 are unpatentable for the reasons set forth in this office action:

INFORMALITIES

2. The proposed drawing correction and/or the proposed substitute sheets of drawings, filed on 7/23/98 have been approved.

DOUBLE PATENTING

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

- A timely filed terminal disclaimer in compliance with 37 CFR 1.321© may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

STAM0041536

4. Claims 87-98,108,110-150 are provisionally rejected under the judicially created doctrine of double patenting over the claims of copending Application No. 08/855561. This is a provisional double patenting rejection since the conflicting claims have not yet
5 been patented.

The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter.

10 Furthermore, there is no apparent reason why applicant would be prevented from presenting claims corresponding to those of the instant application in the other copending application. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

15 5. Claims 87-98,108,110-150 are rejected under the judicially created doctrine of double patenting over claims 1-22 of U. S. Patent No. 5267314 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent

Claims 87-98,108,110-150 are rejected under the judicially created doctrine of double patenting over claims 1-19 of U. S. Patent No. 5524073 since the claims, if
20 allowed, would improperly extend the "right to exclude" already granted in the patent.

Claims 87-98,108,110-150 are rejected under the judicially created doctrine of

double patenting over claims 1-17 of U. S. Patent No. 5555303 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

Claims 87-98,108,110-150 are rejected under the judicially created doctrine of double patenting over claims 1-23 of U. S. Patent No. 5646998 since the claims, if
5 allowed, would improperly extend the "right to exclude" already granted in the patent.

Claims 87-98,108,110-150 are rejected under the judicially created doctrine of double patenting over claims 1-91 of U. S. Patent No. 5793302 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the
10 patent(s) and is covered by the patent(s) since the patent(s) and the application are claiming common subject matter.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See *In re Schneller*, 397 F.2d 350, 158
15 USPQ 210 (CCPA 1968). See also MPEP § 804.

REMARKS


Response to Arguments.

20 The following discussion is introduced in direct response to the arguments presented in the instant amendment:

5

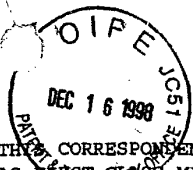
5

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian Zimmerman whose telephone number is (703) 305-4796.


Brian Zimmerman
Patent Examiner
Art Unit 2735

15

STAM0041539



2735

[Handwritten signature]
PATENT

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. McLeod

DATE: 12/14/98

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Attn: Drawing Review
Leon Stambler : Branch
:
Appln. No.: 08/872,116 : Group Art Unit: 2735
:
Filed: June 10, 1997 : Examiner: B. Zimmerman
:
For: METHOD FOR SECURING :
INFORMATION RELEVANT TO A : Attorney Docket
TRANSACTION (as amended) : No. 6074-1U7

RECEIVED

DEC 21 1998

Group 2700

TRANSMITTAL OF FORMAL DRAWINGS
PRIOR TO NOTICE OF ALLOWANCE

Attached please find the formal drawings for this application, consisting of fifteen sheets of drawings, Figs. 1-16. The formal drawings incorporate the changes in the "SUBMISSION OF PROPOSED DRAWING AMENDMENT FOR APPROVAL BY EXAMINER" mailed on November 8, 1996 (filed in the USPTO on November 13, 1996) and the "SUBMISSION OF PROPOSED DRAWING AMENDMENT FOR APPROVAL BY EXAMINER" mailed on July 21, 1998 (filed in the USPTO on July 23, 1998), both of which were previously approved by the Examiner.

Respectfully submitted,

LEON STAMBLER

12/14/98

(Date)

BY:

Clark A. Jablon

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

FIG. 1

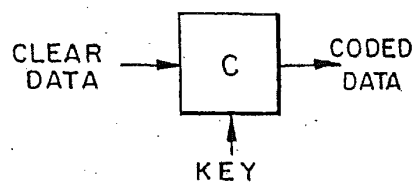


FIG. 2

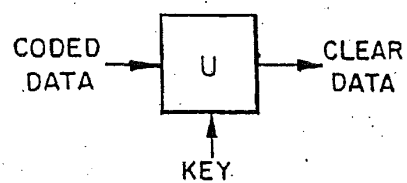


FIG. 3

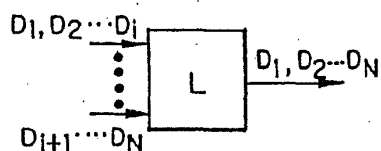


FIG. 4

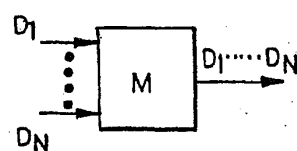


FIG. 5

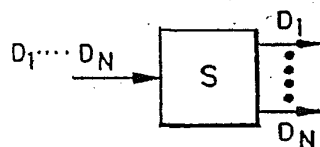
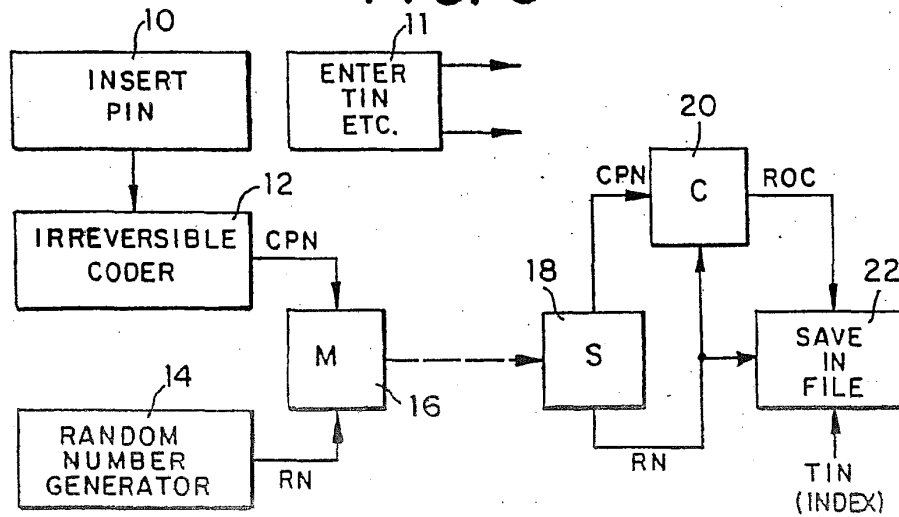


FIG. 6





PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 1 OF 15

RECEIVED
APR 15 1998
Publishing Division
Correspondence

STAM0041543

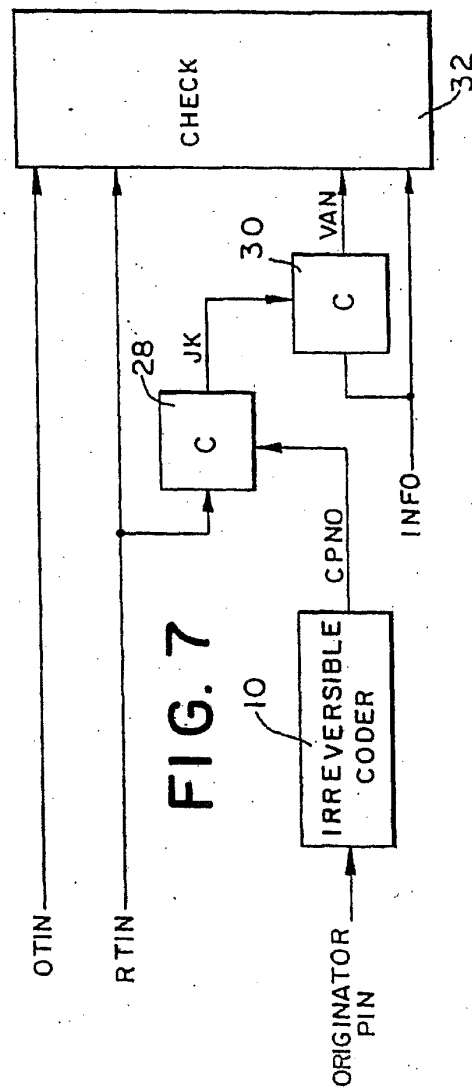


FIG. 7

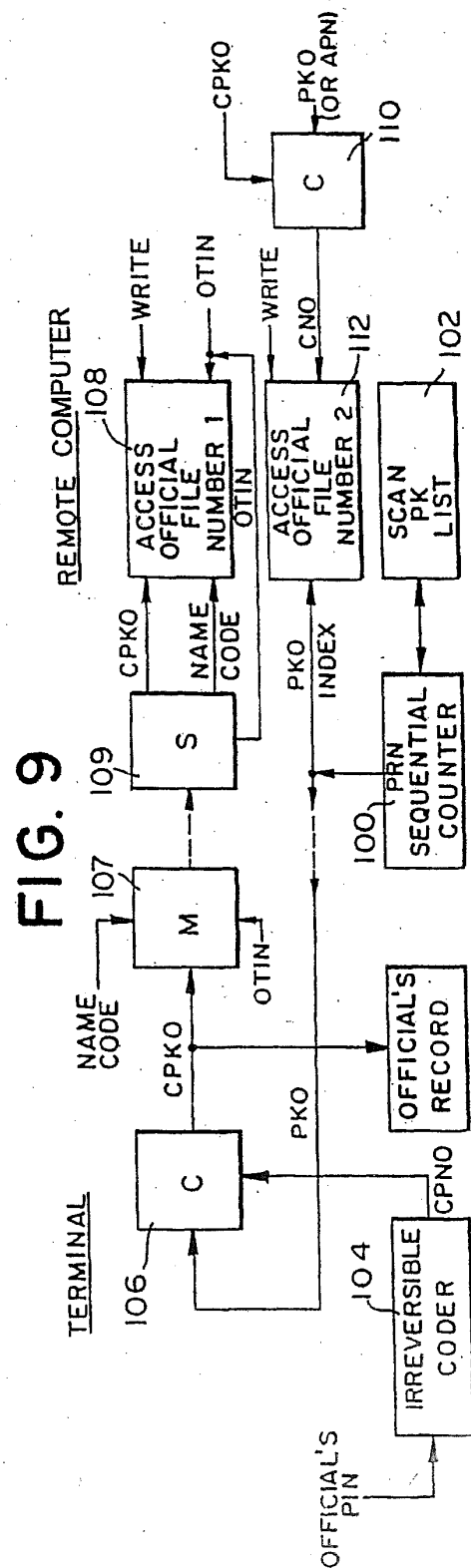


FIG. 9



PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

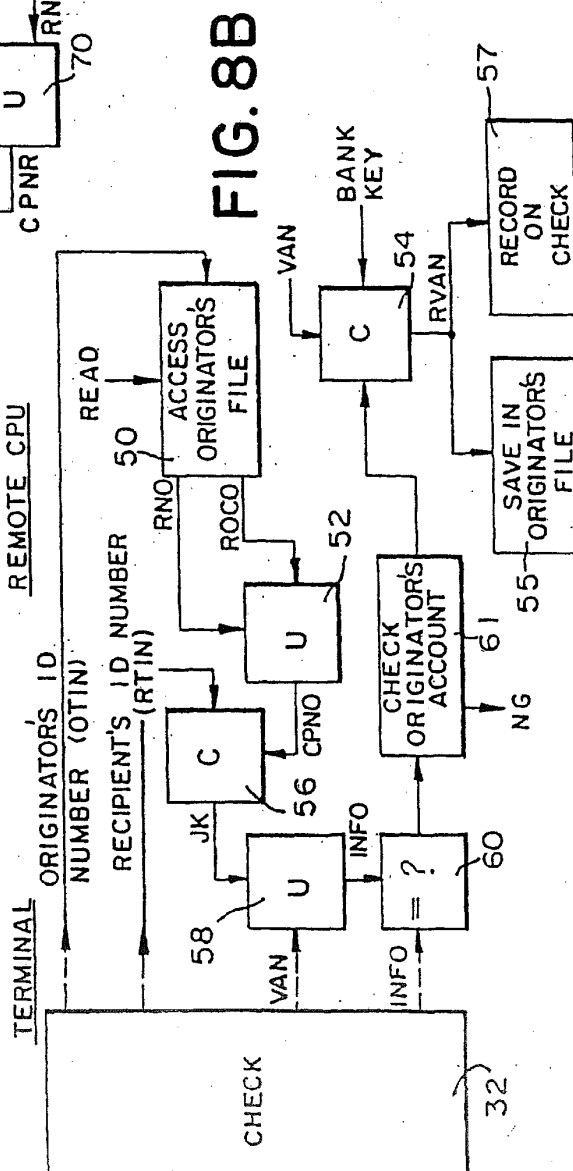
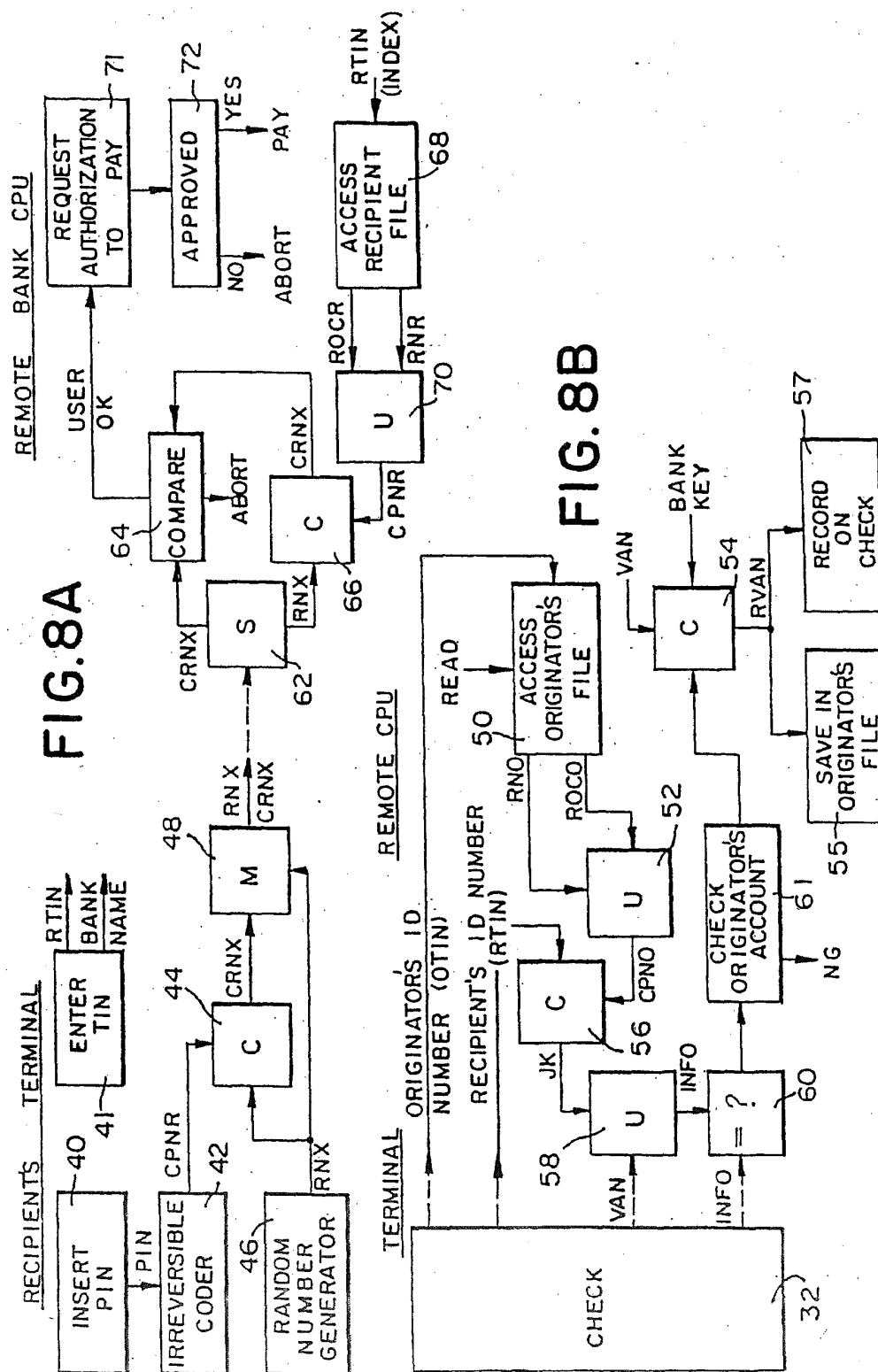
SHEET NO. 2 OF 15

RECEIVED

APR 15 1999

Publishing Division
Correspondence Files (G)

STAM0041545





PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 3 OF 15

RECEIVED

APR 15 1999

Publishing Division
Correspondence

STAM0041547

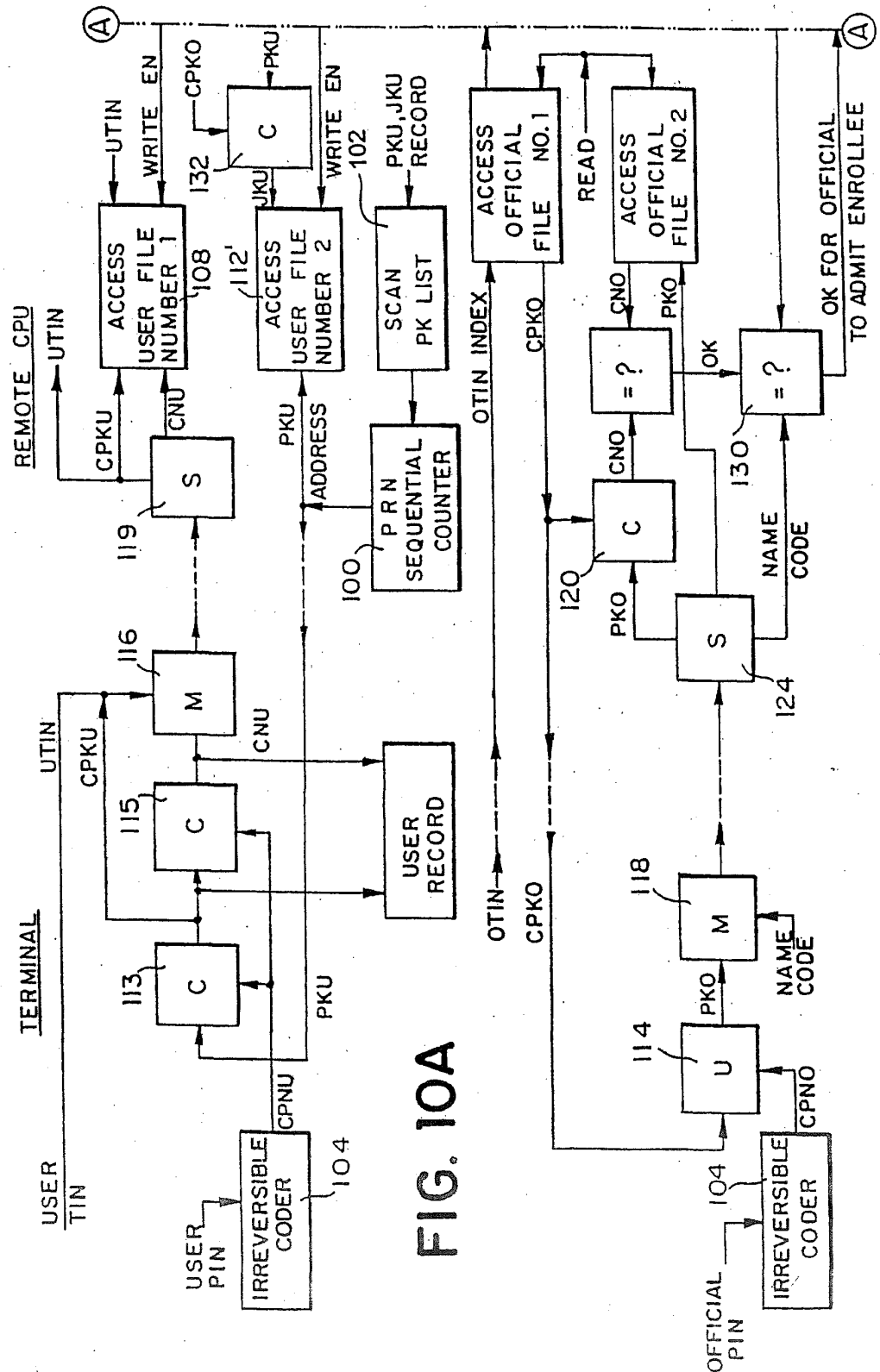


FIG. 10A



PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 4 OF 15

RECEIVED

APR 15 1999

Publishing Division
Correct/Allowed Filed / 5

STAM0041549

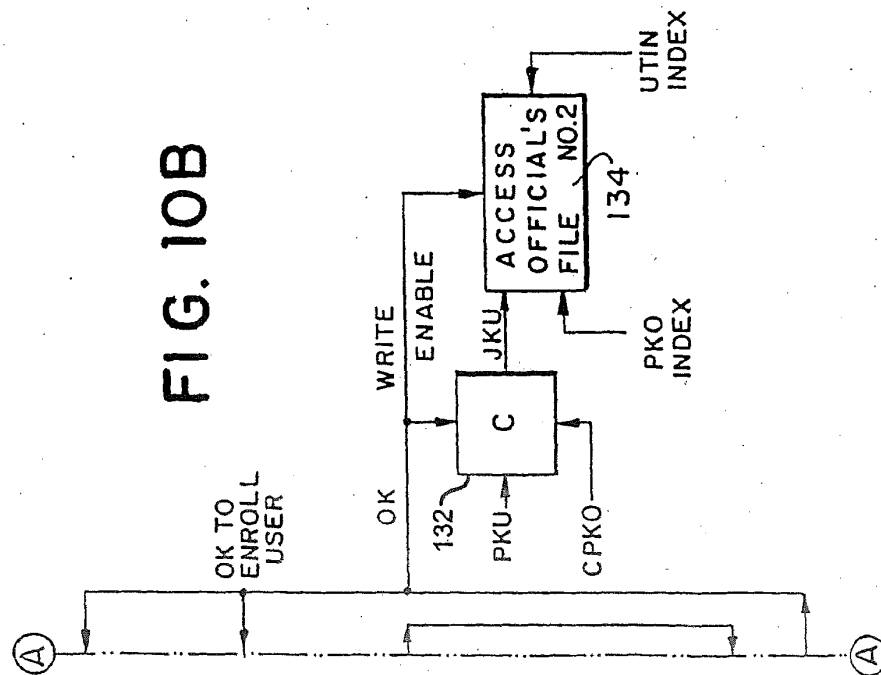


FIG. 10B

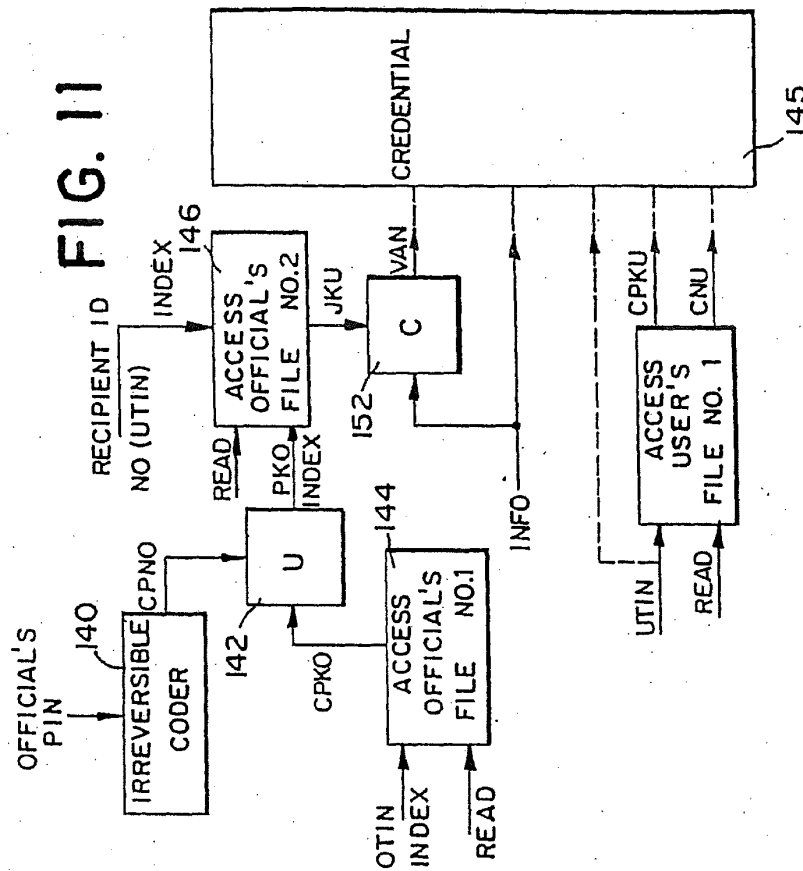


FIG. 11



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

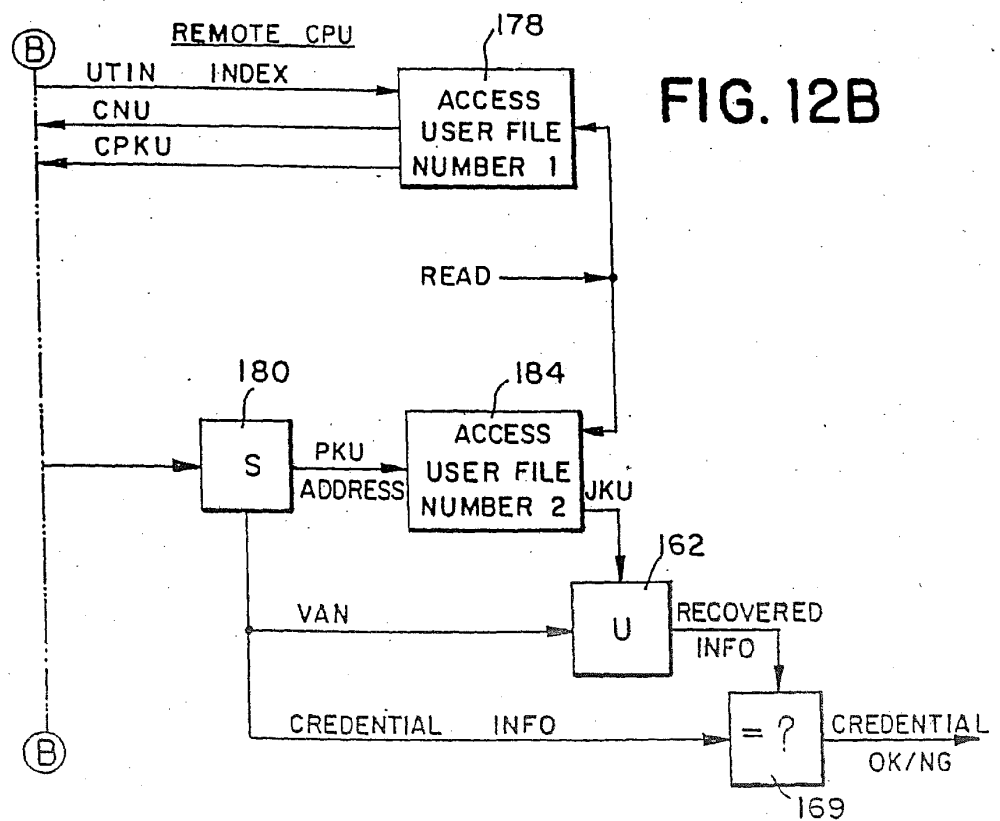
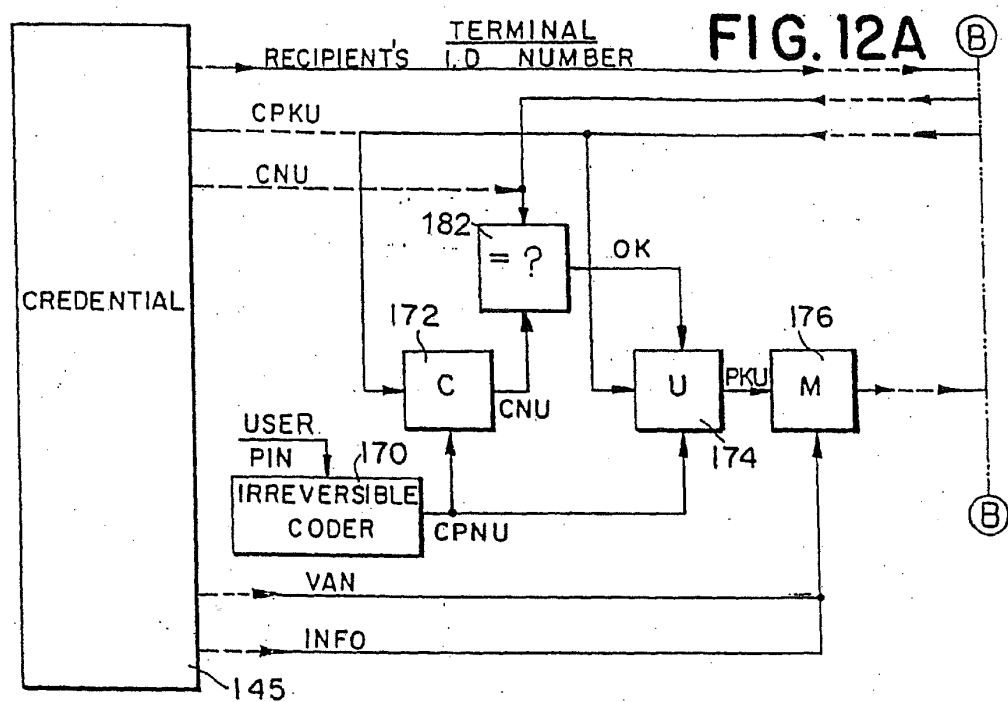
TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 5 OF 15

RECEIVED
APR 15 1999
Publishing Division
Corres/Allowed Entry

STAM0041551



STAM0041552



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

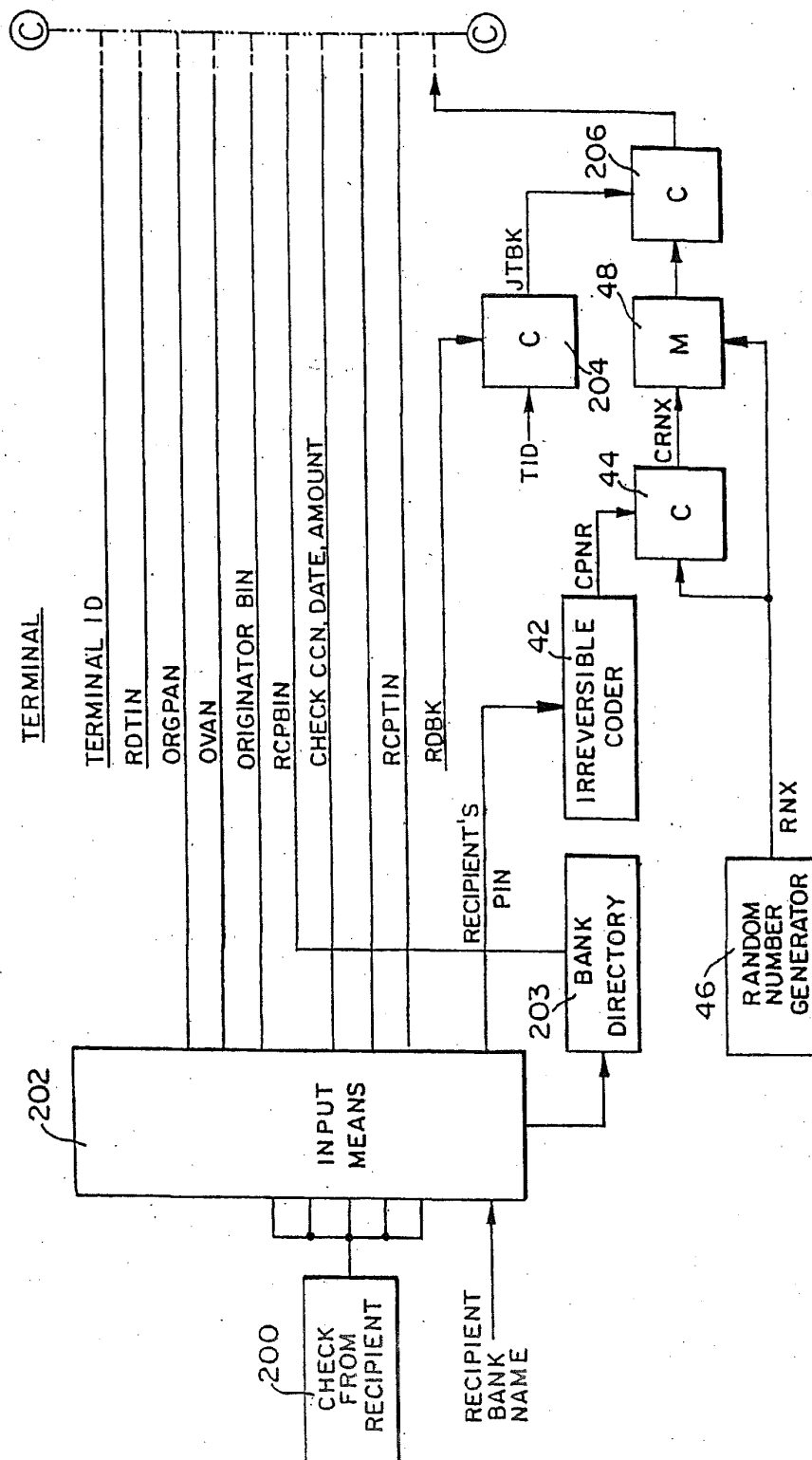
ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 6 OF 15

RECEIVED
APR 15 1999
Publishing Division
Corres/Allowed Files (OT)

STAM0041553

FIG. 13A





PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 7 OF 15

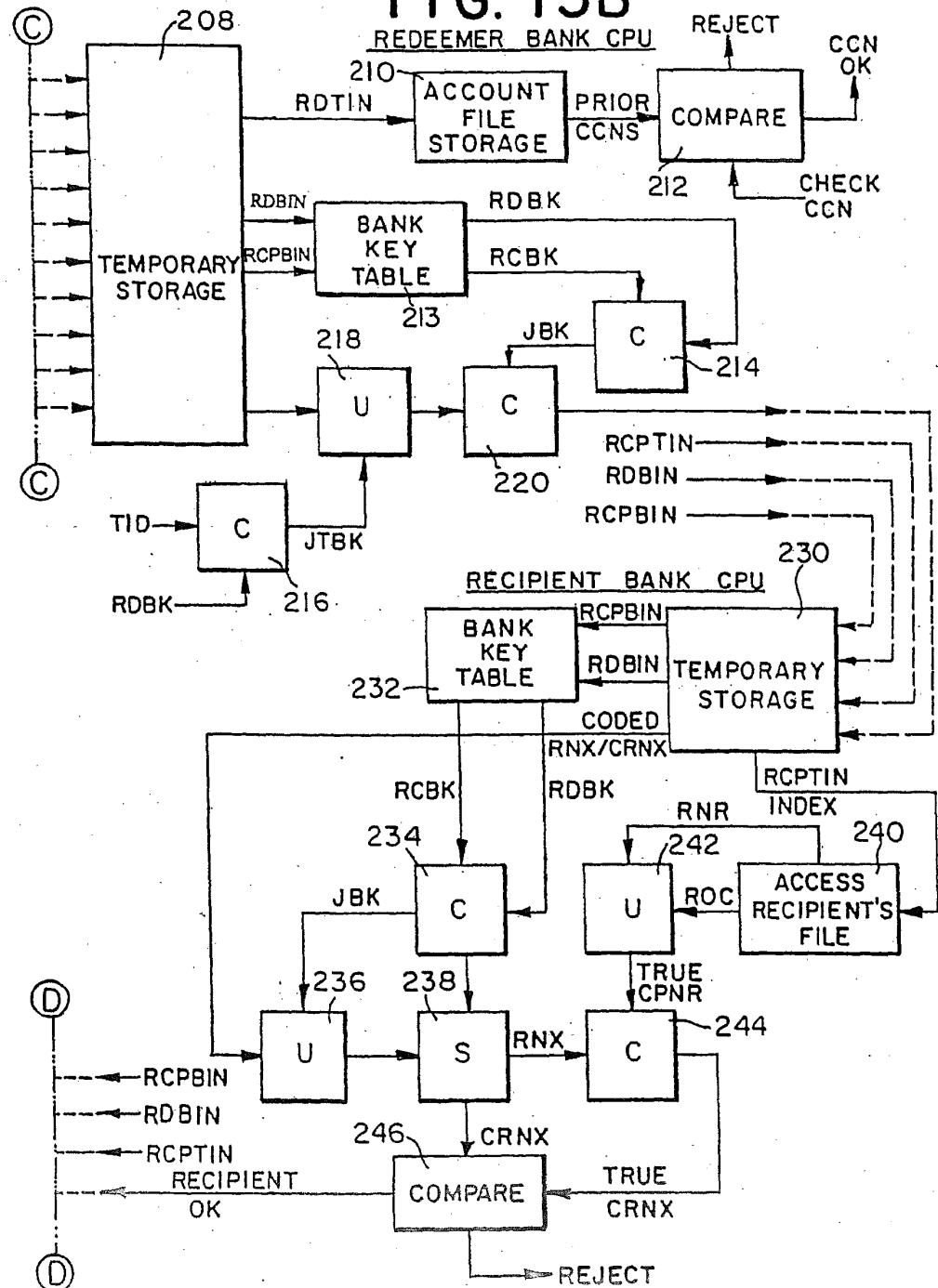
RECEIVED

APR 15 1999

Publishing Division
Corres/Allowed Files

STAM0041555

FIG. 13B





PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 8 OF 15

RECEIVED
APR 15 1999
Publishing Division
Corres/Allowed Files (07)

STAM0041557



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

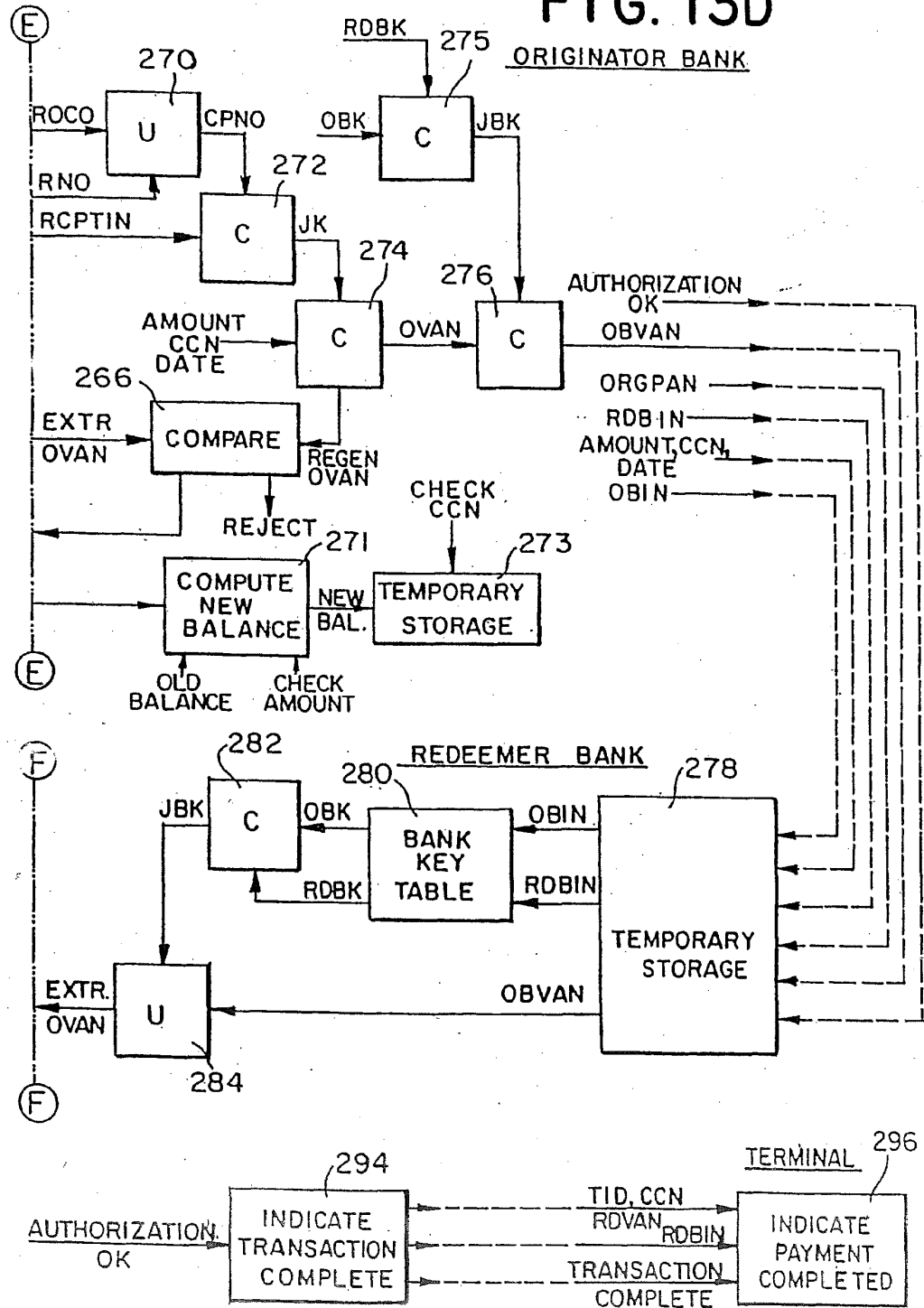
ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 9 OF 15

RECEIVED
APR 15 1999
Publishing Division
Corres/Allowed Files

STAM0041559

FIG. 13D



STAM0041560



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

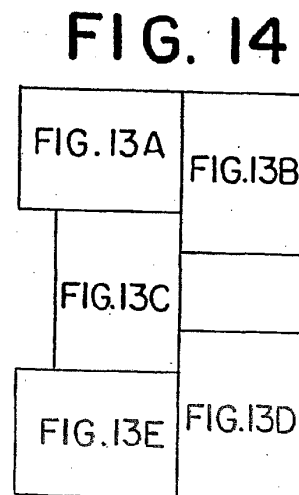
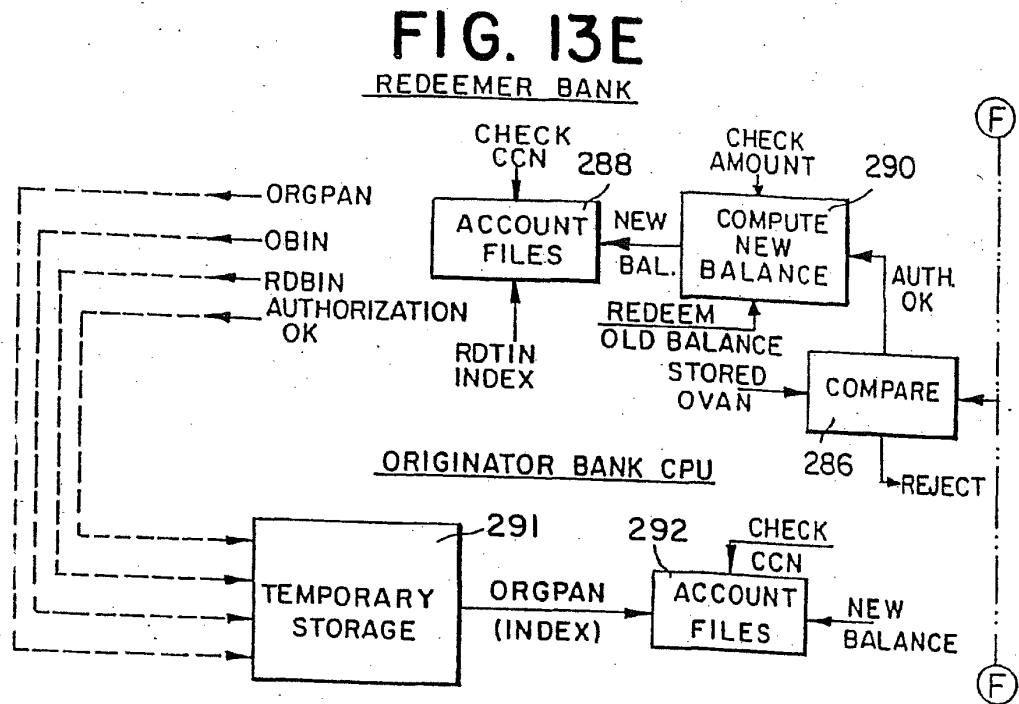
SHEET NO. 10 OF 15

RECEIVED

APR 15 1999

Publishing Division
Corres/Allowed Files (m)

STAM004156'





PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 11 OF 15

RECEIVED
APR 15 1999
Publishing Division
Corres/Allowed

STAM0041563

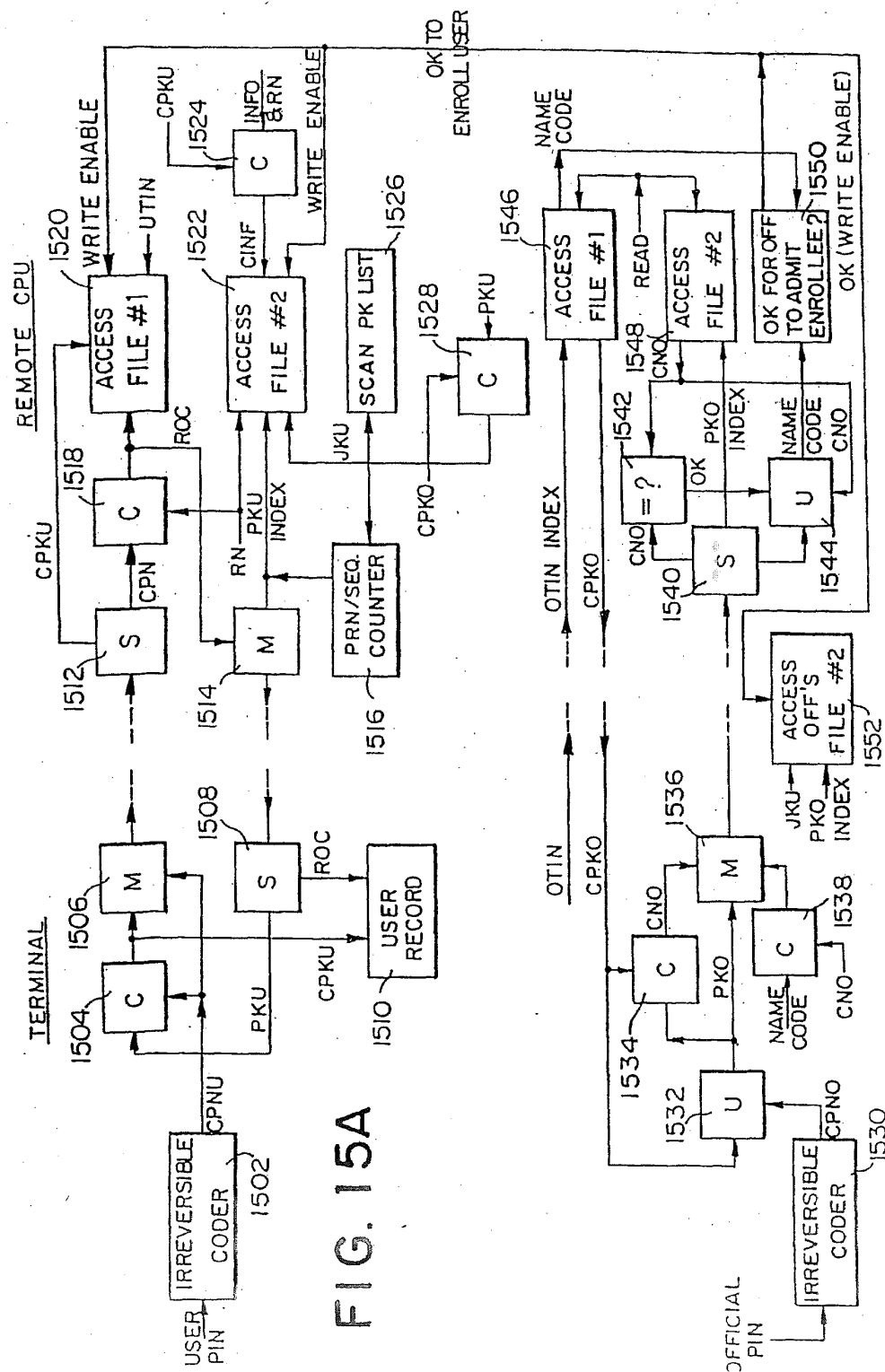


FIG. 15A



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 12 OF 15

RECEIVED
APR 15 1999
Publishing Division
Corres/Allowed Files (07)

STAM0041565

CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL / COMPUTER

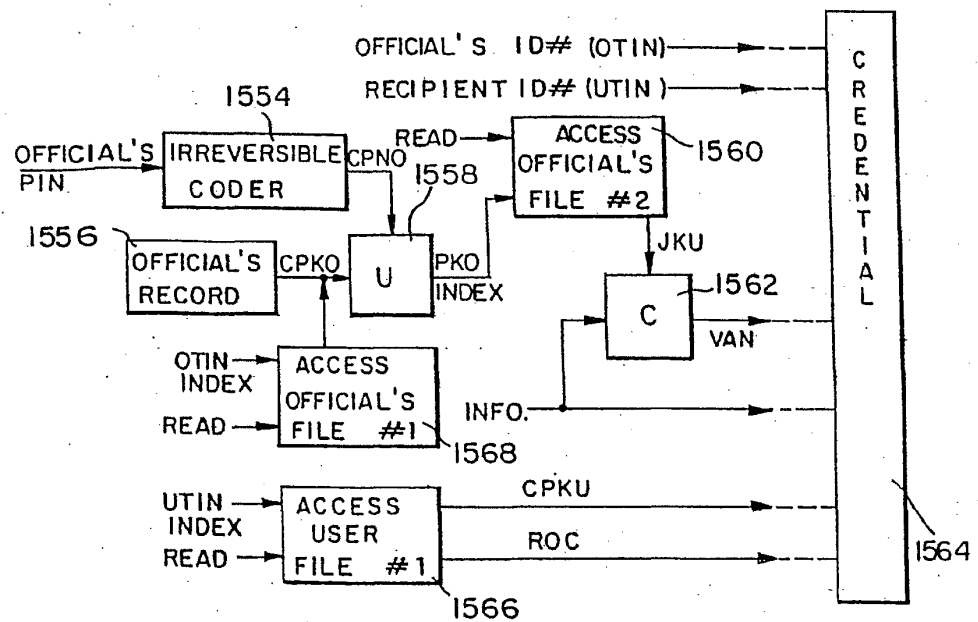


FIG. 15B

STAM0041566



PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 13 OF 15

RECEIVED
APR 15 1999
Publishing Division
Corres/Allowed Files (07)

STAM0041567





PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

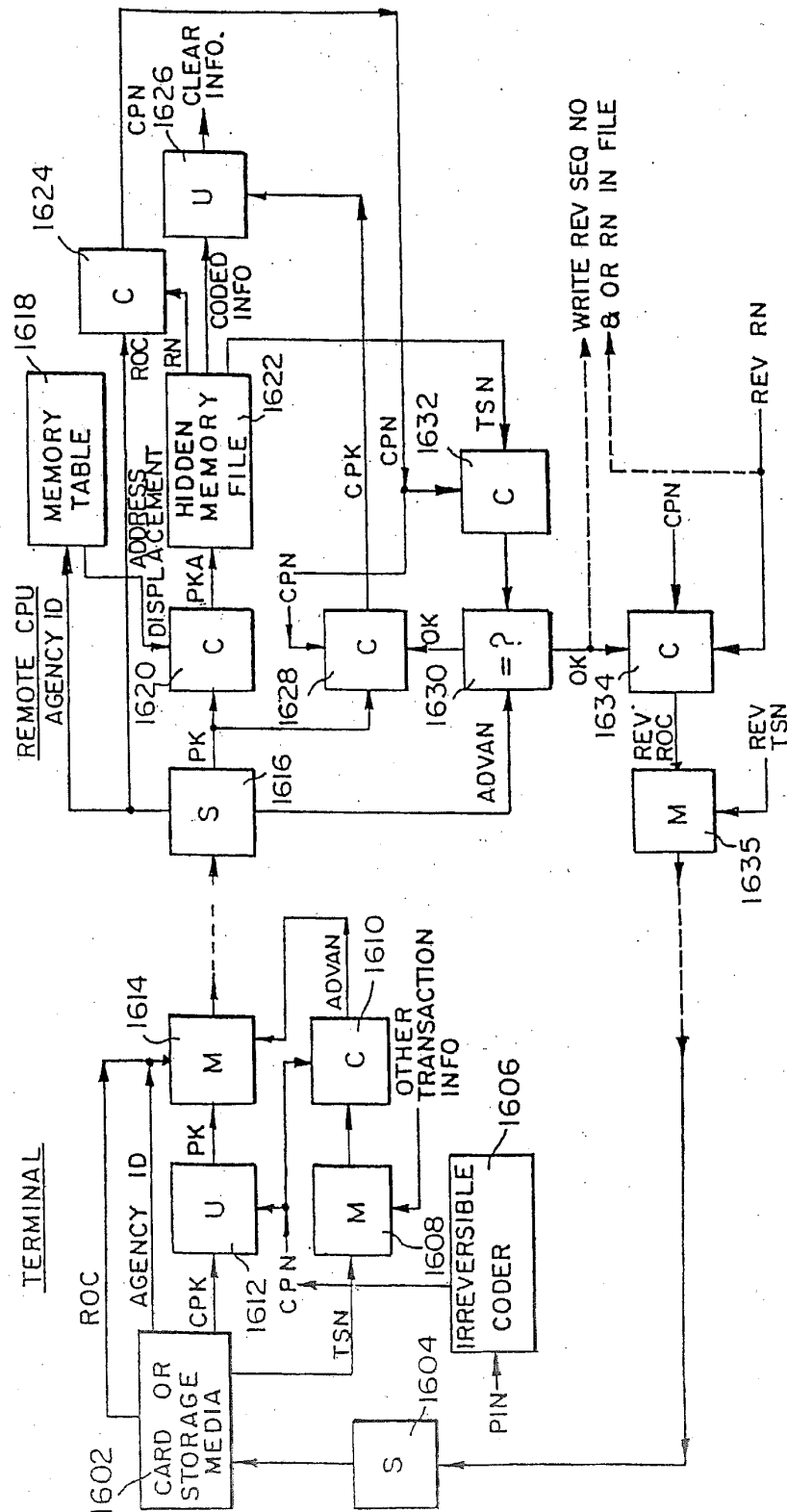
TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 14 OF 15

RECEIVED
APR 15 1999
Publishing Division
Corres/Allowed Files (07)

STAM0041569





PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

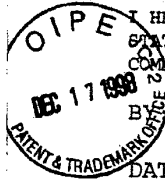
ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 15 OF 15

RECEIVED

APR 15 1999

Publishing Division
Corres/Allowed Files (17



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. of Land
DATE: 12/14/98

2735
1/4
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2735
Leon Stambler :
:
Appln. No.: 08/872,116 : Examiner: B. Zimmerman
:
:
Filed: June 10, 1997 :
:
For: METHOD FOR SECURING :
INFORMATION RELEVANT TO A : Attorney Docket
TRANSACTION (as amended) : No. 6074-1U7

RECEIVED
DEC 24 1998
Group 2700

RESPONSE

This paper is being filed in response to the Office Action mailed September 15, 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 statutory disclaimer fee for presenting the terminal disclaimer.

REMARKS

Claims 87-98, 108 and 110-150 are pending in this application. All of the claims were rejected under double patenting grounds over five of Applicant's related patents and one related pending application.

Double patenting rejections

A terminal disclaimer is provided in response to these rejections. Accordingly, withdrawal of these rejections is respectfully requested.

Formal Drawings

Formal drawings were submitted directly to the Drawing Review Branch concurrently with this paper. The formal drawings incorporate the previously approved changes in the "SUBMISSION OF PROPOSED DRAWING AMENDMENT FOR APPROVAL BY EXAMINER" mailed on November 8, 1996 (filed in the USPTO on November 13, 1996) and the "SUBMISSION OF PROPOSED DRAWING AMENDMENT FOR APPROVAL BY EXAMINER" mailed on July 21, 1998 (filed in the USPTO on July 23, 1998).

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

12/14/98

(Date)

BY:

Clark A. Jablon

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

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. Vifor DATE: 12/14/98



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application of : Group Art Unit: 2735
Leon Stambler :
:
Appln. No.: 08/872,116 : Examiner: B. Zimmerman
:
Filed: June 10, 1997 :
:
For: METHOD FOR SECURING :
INFORMATION RELEVANT TO A : Attorney Docket
TRANSACTION : No. 6074-1U7

RECEIVED

DEC 24 1998

Group 2700

TERMINAL DISCLAIMER TO OBVIATE A
DOUBLE PATENTING REJECTION (37 CFR 1.321(c))

IDENTIFICATION OF PERSON MAKING THIS DISCLAIMER

I, Leslie L. Kasten, Jr. represent that I am a representative authorized to sign on behalf of Leon Stambler, who is the owner of the above-identified unassigned application.

12/22/1998 BLHMS: 00000130 160235 00072116

01 FC:240

55.00 CH

EXTENT OF DISCLAIMANT'S INTEREST

The extent of the interest in this invention that the disclaimant owns is in the whole of this invention.

DISCLAIMER

The owner of the above-identified application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the present application which would extend beyond the expiration date of the full statutory term defined in 35 U.S.C. § 154 to § 156 and § 173 of U.S. Patent Nos. 5,267,314; 5,524,073; 5,555,303; 5,646,998; 5,793,302, as presently shortened by any terminal disclaimer; and any patent granted on U.S. Application No. 08/855,561. The owner of the above-identified application hereby agrees that any patent so granted on the present application shall be enforceable only for and during such period that it and U.S. Patent Nos. 5,267,314; 5,524,073; 5,555,303; 5,646,998; 5,793,302, as presently shortened by any terminal disclaimer; and any patent granted on U.S. Application No. 08/855,561 are commonly owned. This agreement runs with any patent granted on the present application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner of the above-identified application does not disclaim any terminal part of any patent granted on the present application that would extend to the expiration date of the full statutory term defined in 35 U.S.C. § 154 to § 156 and § 173 of the prior patent, in the event that it later: expires for failure to pay a maintenance fee, is held unenforceable or is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or is terminally disclaimed under 37 C.F.R. § 1.321, has all claims canceled by a

re-examination certificate, or is in any manner terminated prior to the expiration of its full statutory term.

FEE STATUS AND PAYMENT
(37 CFR 1.20(d))

This application is entitled to Small Entity status. A verified statement was previously filed in original Application No. 07/977,385 and such status is still proper and desired.

Charge Deposit Account No. 16-0235 in the sum of \$55.00

Also, charge Deposit Account No. 16-0235 for any fee deficiency.

A duplicate of this disclaimer is attached.

Respectfully submitted,

LEON STAMBLER

12/14/98

(Date)

BY: Leslie L. Kasten, Jr.

Leslie L. Kasten, Jr.
Registration No. 28,959
PANITCH SCHWARZE JACOBS & NADEL, P.C.
One Commerce Square
2005 Market Street - 22nd Floor
Philadelphia, PA 19103-7086
Telephone: (215) 567-2020
Facsimile: (215) 567-2991

LLK:CAJ:eam



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/872,116	06/10/97	STAMBLER	L 6074-1U7

000570 LM11/0226
PANITCH SCHWARZE JACOBS & NADEL
ONE COMMERCE SQUARE 22ND FLOOR
2005 MARKET STREET
PHILADELPHIA PA 19103

EXAMINER

ZIMMERMAN, B

ART UNIT	PAPER NUMBER
----------	--------------

2735

#32

DATE MAILED: 02/26/99

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

Commissioner of Patents and Trademarks

STAM0041578



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

NOTICE OF ALLOWANCE AND ISSUE FEE DUE

000570 LM11/0226
PANITCH SCHWARZE JACOBS & NADEL
ONE COMMERCE SQUARE 22ND FLOOR
2005 MARKET STREET
PHILADELPHIA PA 19103

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT	DATE MAILED
08/872,116	06/10/97	054	ZIMMERMAN, B	2735 02/26/99
First Named Applicant	STAMBLER, 35 USC 154(b) term ext. = 0 Days.			

TITLE OF INVENTION: METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2 6074-1U7	340-825.330	P54	UTILITY	YES	\$605.00	05/26/99

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED.

THE ISSUE FEE 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.

HOW TO RESPOND 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 changed, pay twice the amount of the FEE DUE shown above and notify the Patent and Trademark Office of the change in status, or
- B. If the status is the same, pay the FEE DUE shown above.

If the SMALL ENTITY is shown as NO:

A. Pay FEE DUE shown above, or

B. File verified statement of Small Entity Status before, or with, payment of 1/2 the FEE DUE shown above.

II. Part B-Issue Fee Transmittal should be completed and returned to the Patent and Trademark Office (PTO) with your ISSUE FEE. Even if the ISSUE FEE has already been paid by charge to deposit account, Part B Issue Fee Transmittal should be completed and returned. If you are charging the ISSUE FEE to your deposit account, section "4b" of Part B-Issue Fee Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give application number and batch number.

Please direct all communications prior to issuance to Box 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.

PATENT AND TRADEMARK OFFICE COPY

PTOL-65 (REV. 10-96) Approved for use through 05/30/99. (0651-0033)

STAM0041579

Notice of Allowability	Application No. 08/872,116	Applicant(s) Stambler
	Examiner Brian Zimmerman	Group Art Unit 2735

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 and Issue Fee Due or other appropriate communication will be mailed in due course.

☒ This communication is responsive to The terminal disclaimer filed 12/17/98.

☒ The allowed claim(s) is/are 87-98, 108, and 110-150.

☐ The drawings filed on _____ are acceptable.

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

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been
☐ received.
☐ received in Application No. (Series Code/Serial Number) _____
☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

A SHORTENED STATUTORY PERIOD FOR RESPONSE to comply with the requirements noted below is set to EXPIRE **THREE MONTHS** FROM THE "DATE MAILED" of this Office action. Failure to timely comply will result in ABANDONMENT of this application. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

☐ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION, PTO-152, which discloses that the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.

☒ Applicant MUST submit NEW FORMAL DRAWINGS

☐ because the originally filed drawings were declared by applicant to be informal.
☒ including changes required by the Notice of Draftsperson's Patent Drawing Review, PTO-948, attached hereto or to Paper No. 4.
☐ including changes required by the proposed drawing correction filed on _____, which has been approved by the examiner.
☐ including changes required by the attached Examiner's Amendment/Comment.


Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the reverse side of the drawings. The drawings should be filed as a separate paper with a transmittal letter addressed to the Official Draftsperson.

☐ Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Any response to this letter should include, in the upper right hand corner, the APPLICATION NUMBER (SERIES CODE/SERIAL NUMBER). If applicant has received a Notice of Allowance and Issue Fee Due, the ISSUE BATCH NUMBER and DATE of the NOTICE OF ALLOWANCE should also be included.

Attachment(s)

☐ Notice of References Cited, PTO-892
☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____
☐ Notice of Draftsperson's Patent Drawing Review, PTO-948
☐ Notice of Informal Patent Application, PTO-152
☐ Interview Summary, PTO-413
☐ Examiner's Amendment/Comment
☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
☐ Examiner's Statement of Reasons for Allowance


BRIAN ZIMMERMAN
 PRIMARY EXAMINER
 ART UNIT 2735

Complete and mail this form, together with applicable fees, to:

PART B—ISSUE FEE TRANSMITTAL

Box ISSUE FEE
Assistant Commissioner for Patents
Washington, D.C. 20231

\$B

#32

MAILING INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE. Blocks 1 through 4 should be completed where appropriate. All further correspondence including the Issue Fee Receipt, 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: Legibly mark-up with any corrections or use Block 1)

000570 LM11/0226
PANITCH SCHWARZE JACOBS & NADEL
ONE COMMERCE SQUARE 22ND FLOOR
2005 MARKET STREET
PHILADELPHIA PA 19103

Note: The certificate of mailing below can only be used for domestic mailings of the Issue Fee 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.

Certificate of Mailing

I hereby certify that this Issue Fee Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Box Issue Fee address above on the date indicated below.

Darryl Pratcher (Depositor's name)
Darryl Pratcher (Signature)
May 4, 1999 (Date)

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT	DATE MAILED
08/872,116	06/10/97	054	ZIMMERMAN, B	2735 02/26/99
First Named Applicant STAMBLER, 35 USC 154(b) term ext. = 0 Days.				

LE OF
METHOD FOR SECURING INFORMATION RELEVANT TO A TRANSACTION

ATTYS DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2 6074-1U7	340-825.330	P54	UTILITY	YES	\$605.00	05/26/99

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363). Use of PTO form(s) and Customer Number are recommended, but not required.

- ☐ 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) attached.

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. Panitch
2. Schwarze
3. Jacobs + Nadel, P.C.

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. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the PTO or is being submitted under separate cover. Completion of this form is NOT a substitute for an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY & STATE OR COUNTRY)

Please check the appropriate assignee category indicated below (will not be printed on the patent)

- ☐ Individual ☐ corporation or other private group entity ☐ government

4a. The following fees are enclosed (make check payable to Commissioner of Patents and Trademarks):

- ☐ Issue Fee
☐ Advance Order - # of Copies

4b. The following fees or deficiency in these fees should be charged to:

DEPOSIT ACCOUNT NUMBER 16-0235
(ENCLOSE AN EXTRA COPY OF THIS FORM)

- ☒ Issue Fee
☒ Advance Order - # of Copies 10

The COMMISSIONER OF PATENTS AND TRADEMARKS IS requested to apply the Issue Fee to the application identified above.

(Authorized Signature) [Signature] (Date) 5/4/99
NOTE: The Issue Fee 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 Patent and Trademark Office.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending on the needs of the individual case. Any comments on the amount of time required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND FEES AND THIS FORM TO: Box Issue Fee, Assistant Commissioner for Patents, Washington D.C. 20231

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.

05/11/1999 RECEIVED 00000004 160235 00072116

01 FEE
02 FEE

005.00
20.00

RECEIVED

MAY 12 1999

TRANSMIT THIS FORM WITH FEE

PTOL-85B (REV.10-95) Approved for use through 06/30/99. OMB 0551-0033

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

STAM0041581



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER OF
PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	ATTORNEY DOCKET NO.
08/872116	06/10/97	6074-1u7

EXAMINER	
BRIAN ZIMMERMAN	
ART UNIT	PAPER NUMBER
2735	33

DATE MAILED:

Please find below a communication from the Examiner in charge of this application.

Commissioner of Patents and Trademarks

The Supplemental Declaration filed 4/1/99 has been received and entered.


BRIAN ZIMMERMAN
PRIMARY EXAMINER

STAM0041582

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, DC 20231, ON THE DATE INDICATED BELOW



Sheryl R. Neumann

DATE: March 30, 1999

BOX ISSUE FEE
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Office of Publications
Leon Stambler :
Appln. No.: 08/872,116 : Batch No.: P54
Filed: June 10, 1997 : Allowed: February 26, 1999
For: METHOD FOR SECURING INFORMATION : Attorney Docket
RELEVANT TO A TRANSACTION : No. 6074-1U7

RECEIVED

MAR 30 1999

Publishing Unit
Corres/Allowed Files (02)

TRANSMITTAL LETTER

Although it is Applicant's opinion that the claims filed by way of amendment are substantially embraced in the statement of invention or in the claims originally filed, Applicant herewith file(s) a Supplemental Declaration for precautionary purposes under 37 CFR 1.67.

Respectfully submitted,

LEON STAMBLER

3/30/99
(Date)

By:

Clark A. Jablon

CLARK A. JABLON
Registration No. 35,039
PANTICH 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
E-Mail: psjn@psjn.com

CAJ/srn
Enclosure

PSJN2/222757.1

STAM0041583



Attorney Docket No. 6074-1U7

SUPPLEMENTAL DECLARATION
(Related Application)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed, as amended by any and all amendments entered during the prosecution of the patent application identified herein, and for which a patent is sought on the invention entitled **Method For Securing Information Relevant To A Transaction** the specification of which was filed on **June 10, 1997** as Application No. **08/872,116**.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any and all amendments entered during the prosecution of the application identified herein and during the prosecution of the related patent applications identified below.

I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application(s) in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose information material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

<u>08/446,369</u> (Application No.)	<u>May 22, 1995</u> (Filing Date)	<u>Abandoned</u> (Status-patented, pending, abandoned)
<u>08/122,071</u> (Application No.)	<u>September 14, 1993</u> (Filing Date)	<u>Patented</u> (Status-patented, pending, abandoned)
<u>07/977,385</u> (Application No.)	<u>November 17, 1992</u> (Filing Date)	<u>Patented</u> (Status-patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issues thereon.

Full name of sole or
first inventor Leon Stambler

Inventor's Signature Leon Stambler

Date 03/25/99

Residence Parkland, Florida

Citizenship United States of America

Post Office
Address 7803 Boulder Lane
Parkland, Florida 33067



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/872,116	06/10/97	STAMBLER	L 6074-1U7

Q00570 LM11/0512
PANITCH SCHWARZE JACOBS & NADEL
ONE COMMERCE SQUARE 22ND FLOOR
2005 MARKET STREET
PHILADELPHIA PA 19103

EXAMINER
ZIMMERMAN, B

ART UNIT PAPER NUMBER
2735 34

DATE MAILED:05/12/99

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

Commissioner of Patents and Trademarks

75FO/ 409-90
93 7510
B #35JW

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:

Louisa Drain

DATE:

April 12, 1999



PATENT

BOX ISSUE FEE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of
Leon Stambler

: ATTN: OFFICIAL DRAFTSPERSON

Appln. No.: 08/872,116

: Allowed: February 26, 1999

Filed: June 10, 1997

: Batch No. P54

For: METHOD FOR SECURING
INFORMATION RELEVANT TO A
TRANSACTION

: Attorney Docket
: No. 6074-1U7

RECEIVED

APR 15 1999

Publication Division
Corres/Allowed Files (07)

COMMUNICATION REGARDING FORMAL DRAWINGS

No formal drawings are believed to be due for the above-identified patent application. The Notice of Allowability stating that formal drawings are required is believed to be in error, as explained below.

On December 14, 1998, a "Transmittal of Formal Drawings Prior to Notice of Allowance" along with 15 sheets of formal drawings (copies attached herewith), was mailed under separate cover addressed to the "Drawing Review Branch" of the USPTO. The postcard mailed with the above-mentioned Transmittal was returned, date-stamped for receipt by the USPTO: "DEC 16 1998". A copy of the date-stamped postcard is enclosed.

In the Response mailed on December 14, 1998 (filed in the USPTO on December 17, 1999), it was requested that the Examiner indicate whether the formal drawings are acceptable. Unfortunately, the Examiner did not indicate on the Notice of Allowability whether the formal drawings were received or were found acceptable. Phone calls made to the Drafting

PSJN2/224988.1

-1-

STAM0041588

Branch have been unsuccessful in determining whether the formal drawings were reviewed and/or approved. Accordingly, it is requested that the enclosed copy of the previously filed formal drawings be reviewed and approved if the original set of previously filed formal drawings have not been reviewed and approved.

Applicant's undersigned attorney believes these formal drawings place this application in condition for publication of the Letters Patent.

Please telephone Applicant's undersigned attorney if additional information or materials are needed to resolve any of the outstanding issues.

Respectfully submitted,

LEON STAMBLER

4/12/99 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

CAJ:lcd



LAJ/gam

ATTORNEY DOCKET # 6074-107 TODAY'S MAILING DATE 12/14/98

PAT/TM/S. N. / REG/OPP/CANC./# 08/872, 116

CERT. of MAIL/CERT. of SERV/EXPRESS MAIL

OF: Leone, Stanley

FOR: Methods for securing information...

RECEIPT IS ACKNOWLEDGED FOR THE FOLLOWING:

TRADEMARK APPLICATION	COVER SHEET/LETTER/ORDER
Specimens	AMENDMENT/REQ. RECONS
RENEWAL/AFF 8/AFF 8 & 15	ASSIGN/CHG NAME/MERGER/SEC. INT.
PAT APP (NEW/DIV/CIP/RWC/RE)	VER STMT/SMALL ENTITY
Dec & Power of Atty	NOTICE OF APPEAL/BRIEF _____ COPIES
Pages Specifications	FINAL FEE
Preliminary Amendment	SUPPL. DECL _____
Claims	INF. DISCL STATEMENT _____
Sheets Drawings	PRIORITY DOC. _____
Type _____	PET/MOT. FOR EXT. TIME _____

Fee authorization charge TRADE #16-0235 \$ 55.00

OTHER (PAPER TITLE) Response to Terminal Disclaimer
to Abrate a Double Patenting Rejection

872116
07446369

FIG. 1

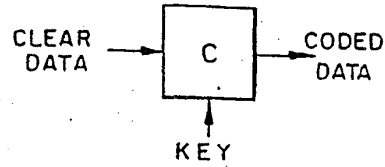


FIG. 2

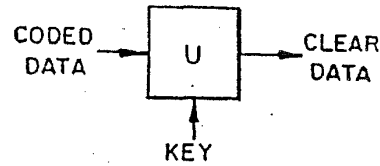


FIG. 3

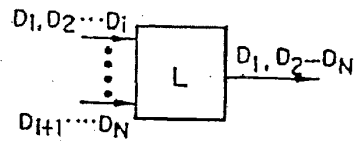


FIG. 4

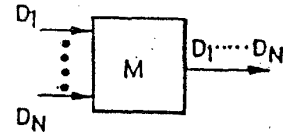


FIG. 5

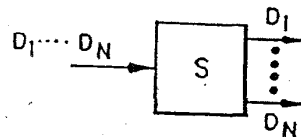
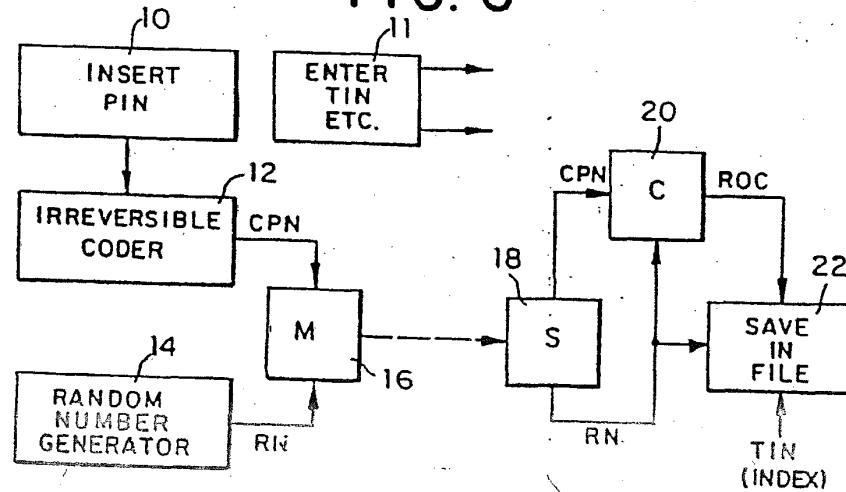


FIG. 6



000000



RECEIVED
GENERAL
MAIL

STAM0041592

872116
44369

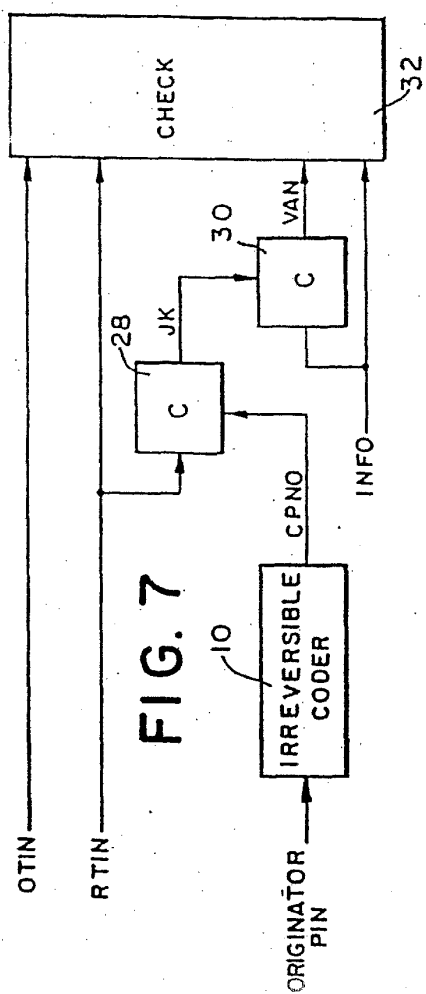
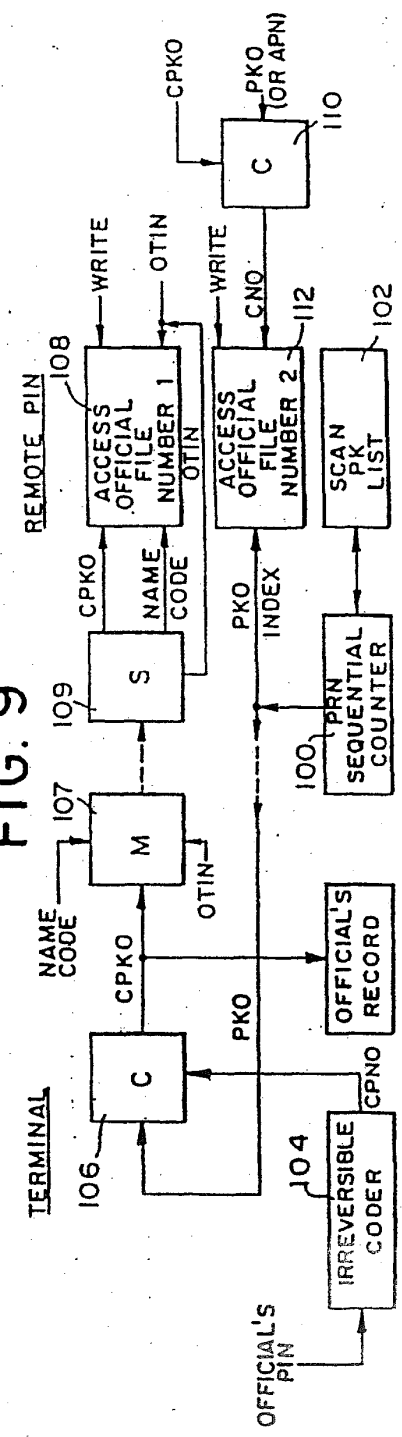


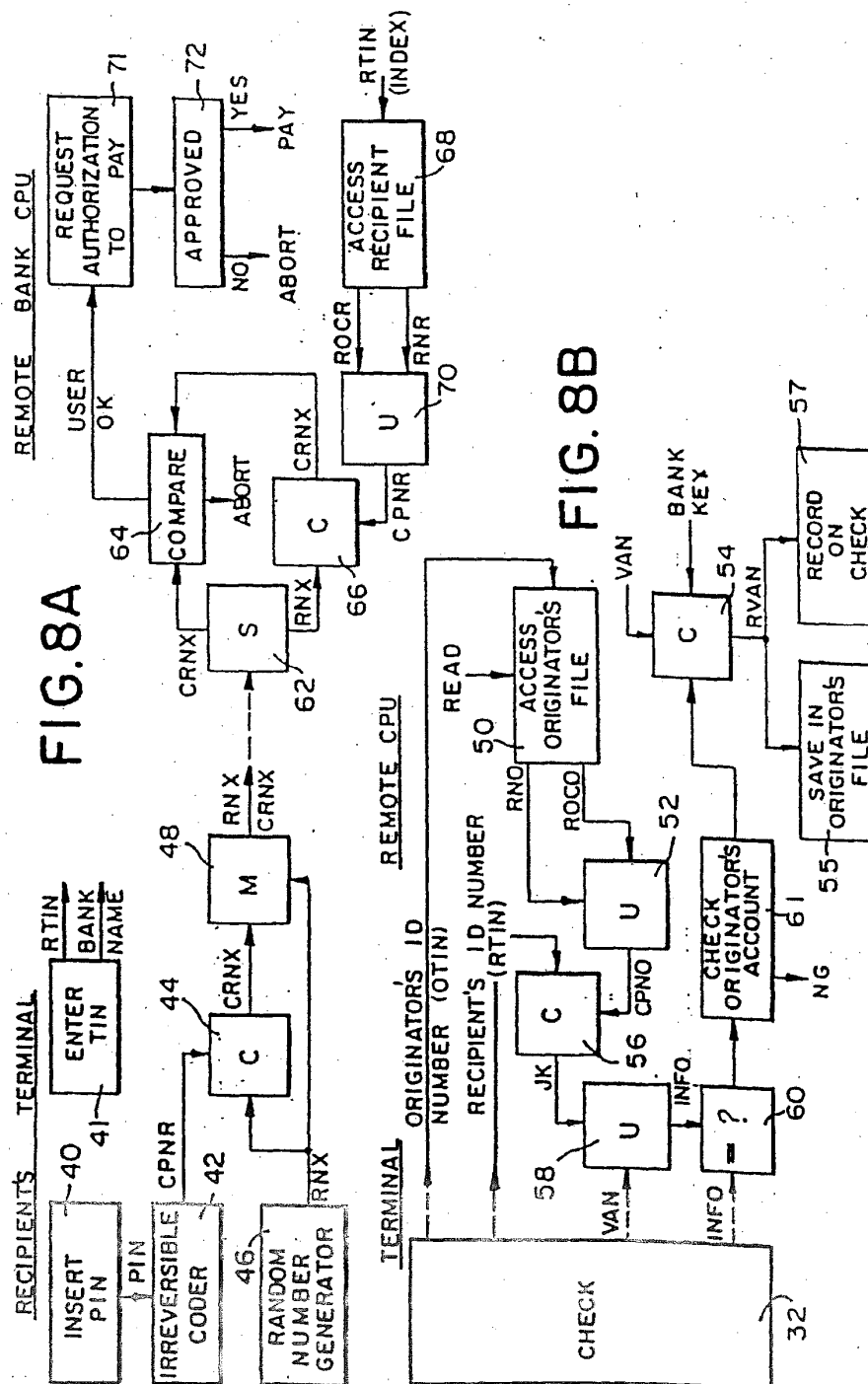
FIG. 7

FIG. 9





872116







STAM0041598

FIG. 10B

The diagram shows a system with a central horizontal bus. On the left, a signal line labeled (A) enters the bus. A signal labeled "OK TO ENROLL USER" is connected to the bus. A signal labeled "OK" is connected to the bus. A signal labeled "WRITE" is connected to the bus. A signal labeled "ENABLE" is connected to the bus. A signal labeled "JKU" is connected to the bus. A signal labeled "PKU" is connected to the bus. A signal labeled "CPKU" is connected to the bus. A signal labeled "PKO INDEX" is connected to the bus. A signal labeled "UTIN INDEX" is connected to the bus. A signal labeled "ACCESS OFFICIAL'S FILE NO.2" is connected to the bus. A signal labeled "134" is connected to the bus. A signal labeled (A) exits the bus on the right.

OK TO ENROLL USER

OK

WRITE

ENABLE

JKU

PKU

CPKU

PKO INDEX

ACCESS OFFICIAL'S FILE NO.2

134

UTIN INDEX

(A)

(A)

॥७॥

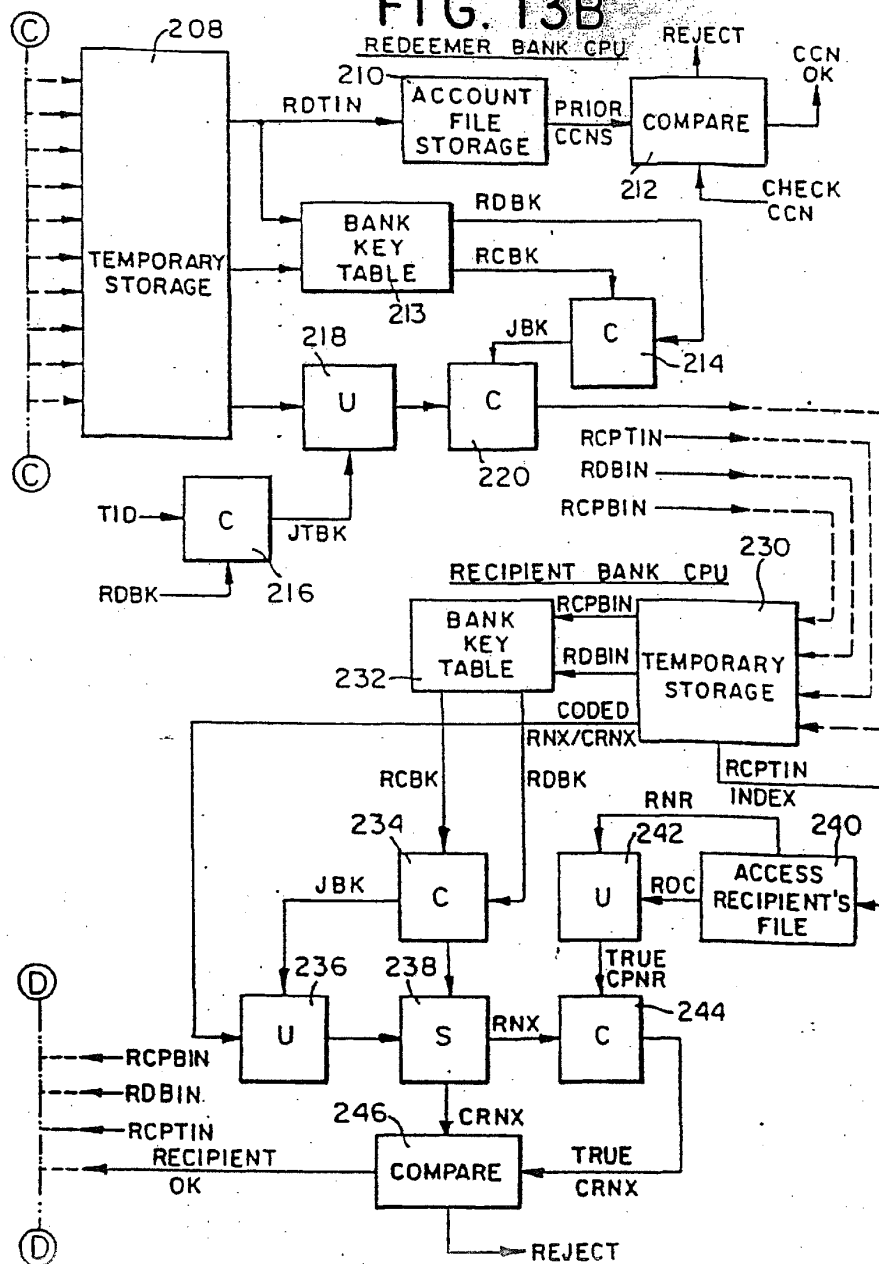






872116
17446869

FIG. 13B

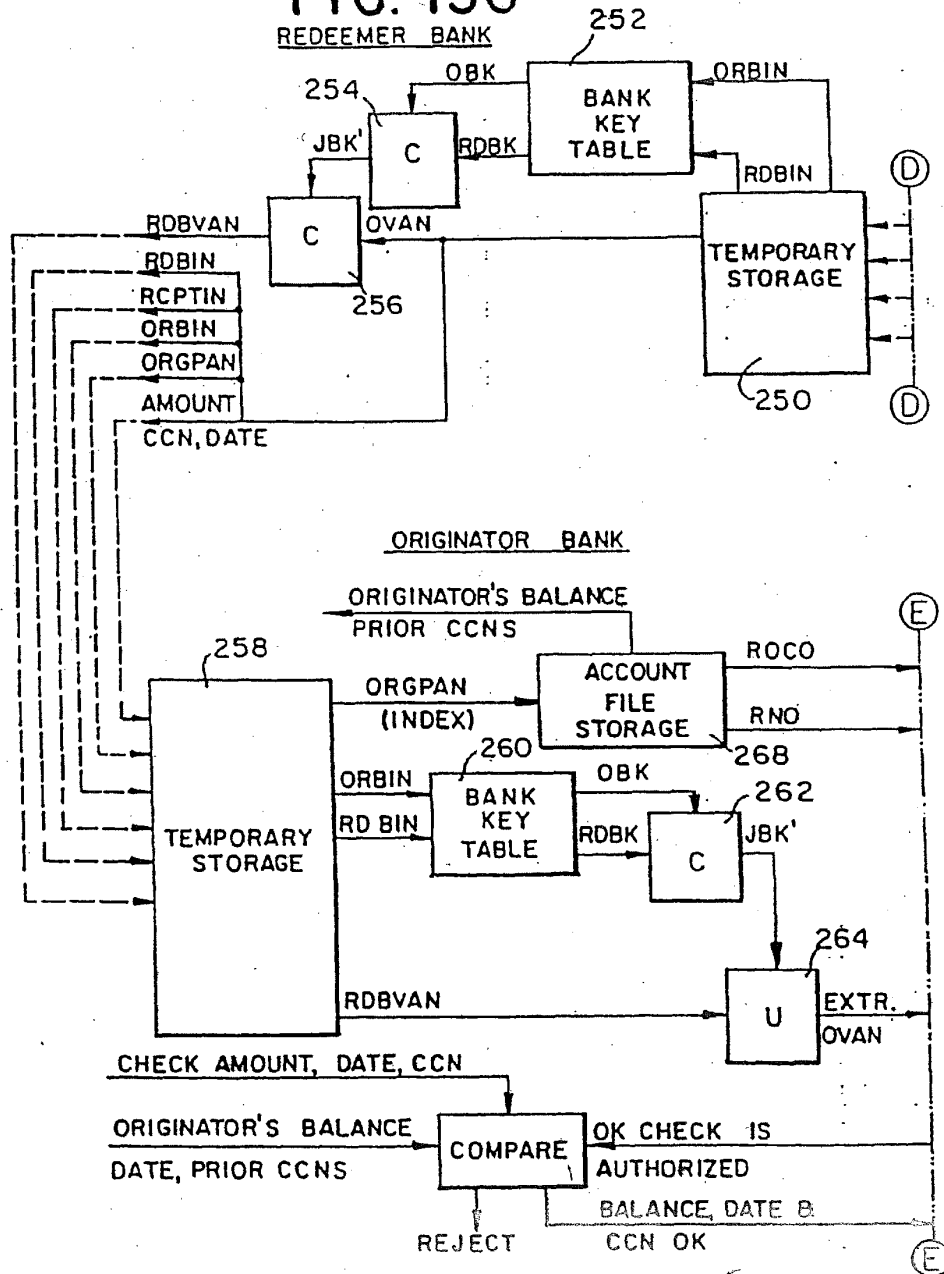




STAM0041606

873,116
 03/13/69

FIG. 13C

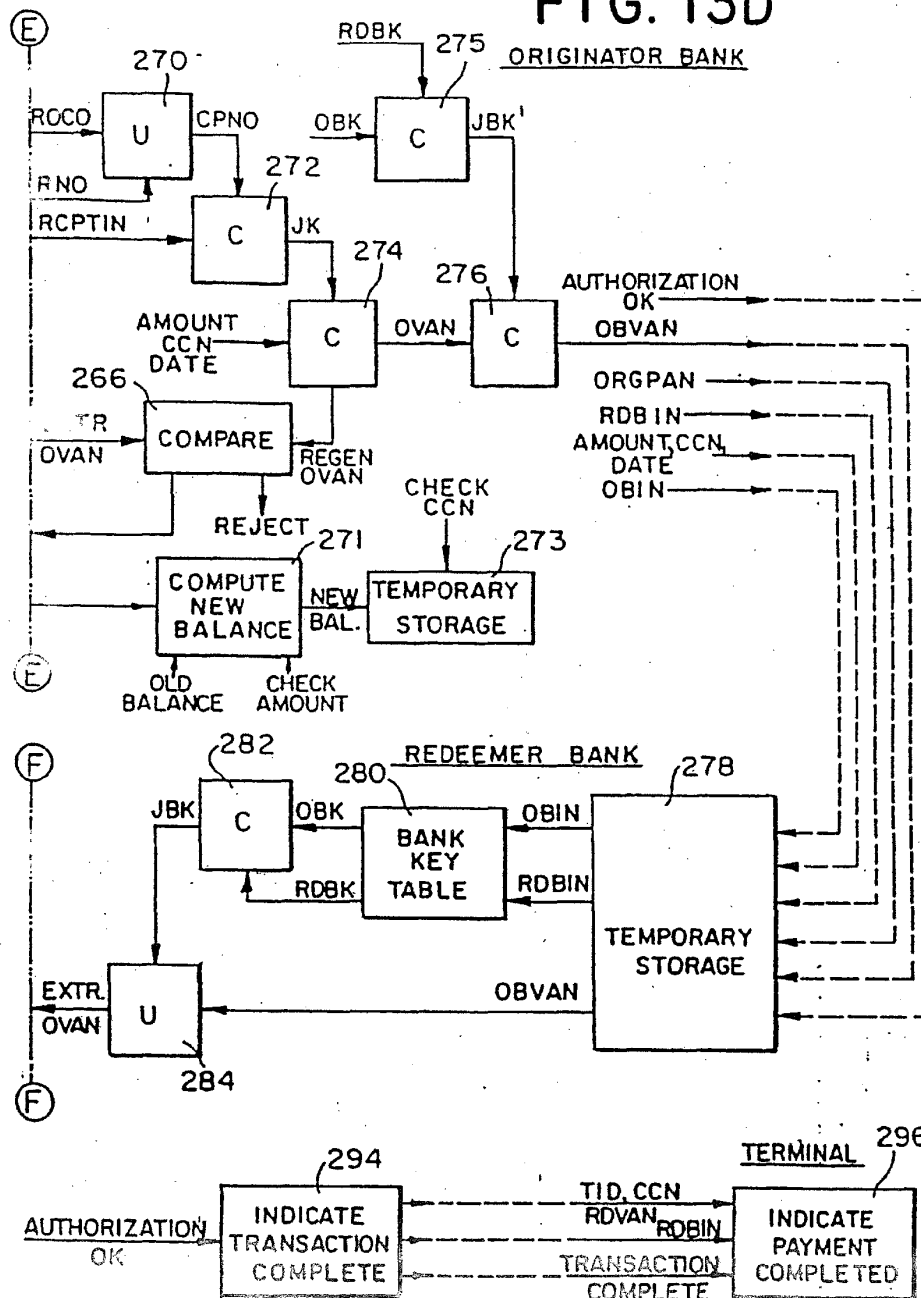




STAM0041608

872116
00/446369

FIG. 13D



STAM0041609

00000000



STAM0041610

87B/16
44663

FIG. 13E

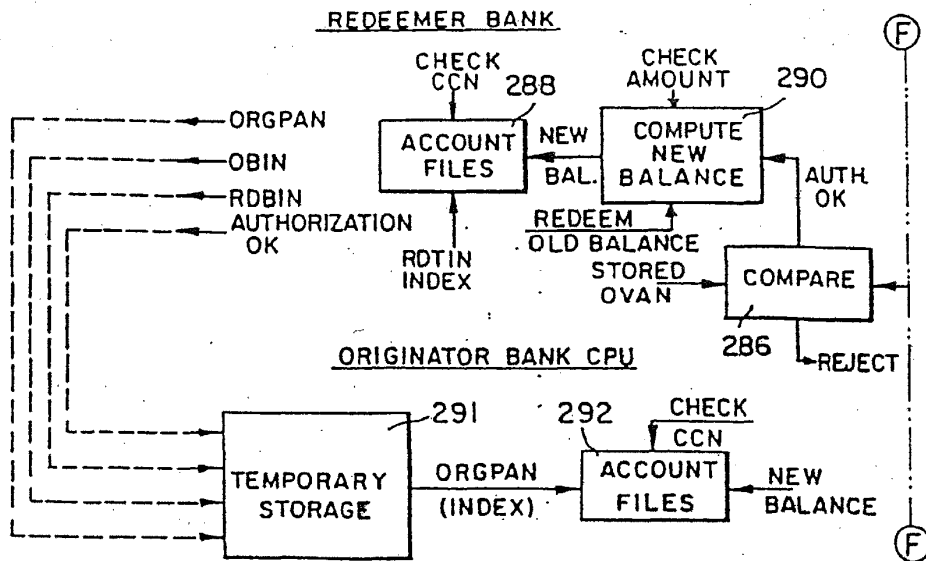
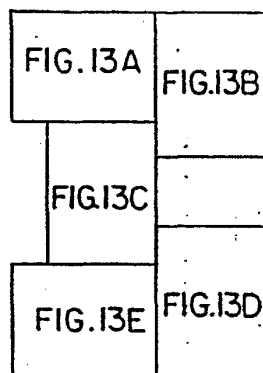


FIG. 14





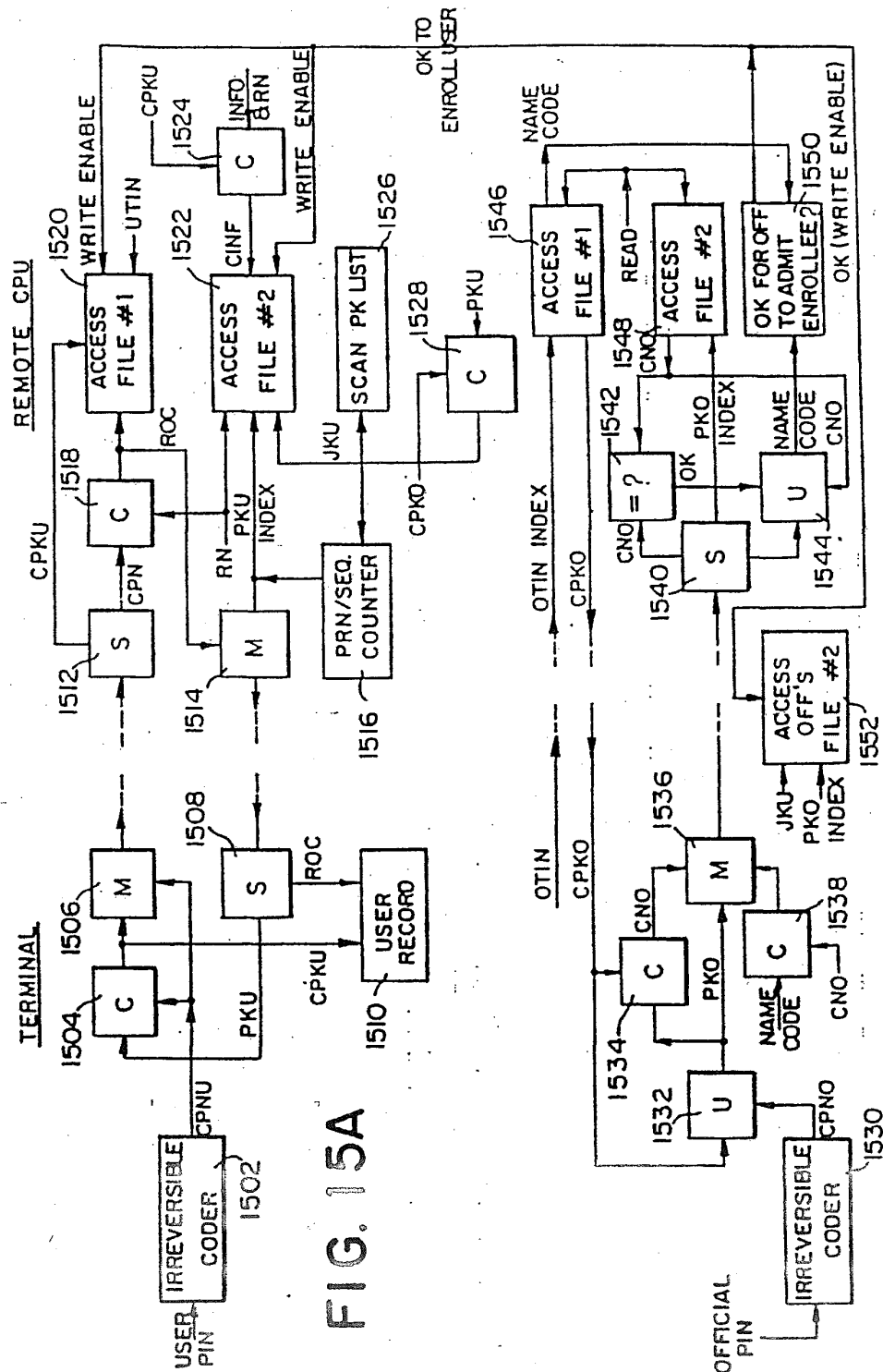


FIG. 15A



872,116
 00/446269

CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL / COMPUTER

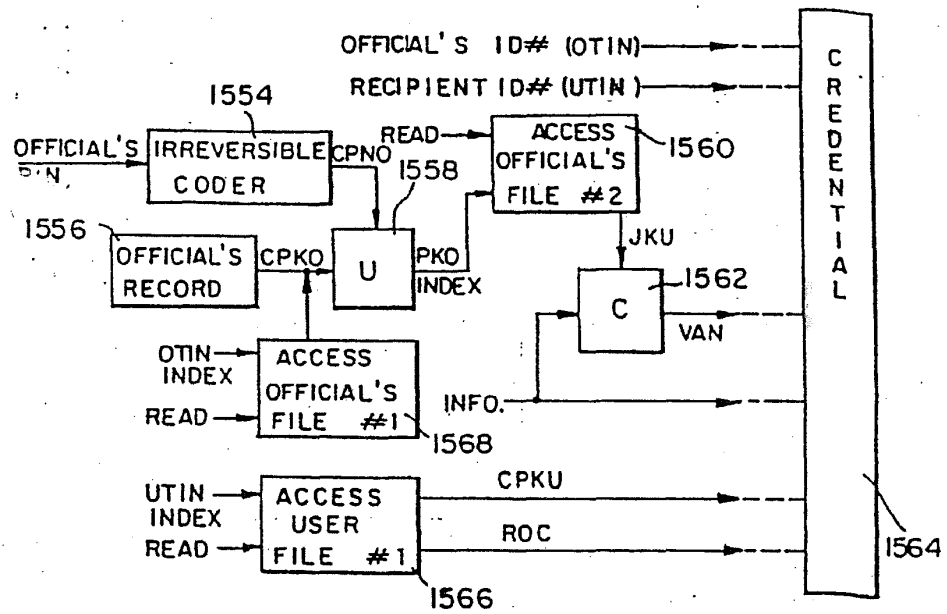


FIG. 15 B

00881X10



STAM0041616

The diagram illustrates a cryptographic system architecture with the following components and data flows:

- Terminal:**
 - Inputs: **USER PIN** (1570), **IRREVERSIBLE CODER** (1572).
 - Block **U** (1574) receives the **USER PIN** and outputs **CPKU** (1574).
 - Block **C** (1574) receives **CPKU** and outputs **CNU** (1574).
 - Block **M** (1576) receives **CNU** and outputs **PKU** (1576).
 - Block **S** (1578) receives **PKU** and outputs **INDEX** (1578).
 - Block **U** (1584) receives **INDEX** and outputs **ROC** (1584).
 - Block **C** (1582) receives **ROC** and outputs **CPKU** (1582).
 - Block **?** (1580) receives **CPKU** and outputs **CNU** (1580).
- Remote CPU:**
 - Block **ACCESS FILE #1** (1588) receives **READ** (1588) and outputs **CPKU** (1588).
 - Block **ACCESS FILE #2** (1586) receives **READ** (1586) and outputs **CPKU** (1586).
 - Block **?** (1580) receives **CPKU** and outputs **CNU** (1580).
- OTIN Official's IO #:**
 - Block **ACCESS OFFICIAL FILE #1** (1599) receives **READ** (1599) and outputs **CPKU** (1599).
 - Block **?** (1596) receives **CPKU** and outputs **PKU** (1596).
 - Block **U** (1592) receives **PKU** and outputs **INFO** (1592).
 - Block **?** (1594) receives **INFO** and outputs **CREDENTIAL OK/NG** (1594).
- System-wide Data Flows:**
 - CPKU** (1574) flows from the Terminal to the Remote CPU.
 - CNU** (1574) flows from the Terminal to the Remote CPU.
 - INDEX** (1578) flows from the Terminal to the Remote CPU.
 - ROC** (1584) flows from the Remote CPU to the OTIN Official's IO #.
 - CPKU** (1582) flows from the Remote CPU to the OTIN Official's IO #.
 - CNU** (1580) flows from the Remote CPU to the OTIN Official's IO #.
 - READ** (1588) flows from the Remote CPU to the OTIN Official's IO #.
 - READ** (1586) flows from the Remote CPU to the OTIN Official's IO #.
 - READ** (1599) flows from the OTIN Official's IO # to the Remote CPU.
 - PKU** (1596) flows from the OTIN Official's IO # to the Remote CPU.
 - INFO** (1592) flows from the OTIN Official's IO # to the Remote CPU.
 - CREDENTIAL OK/NG** (1594) flows from the OTIN Official's IO # to the Remote CPU.

FIG. 15C



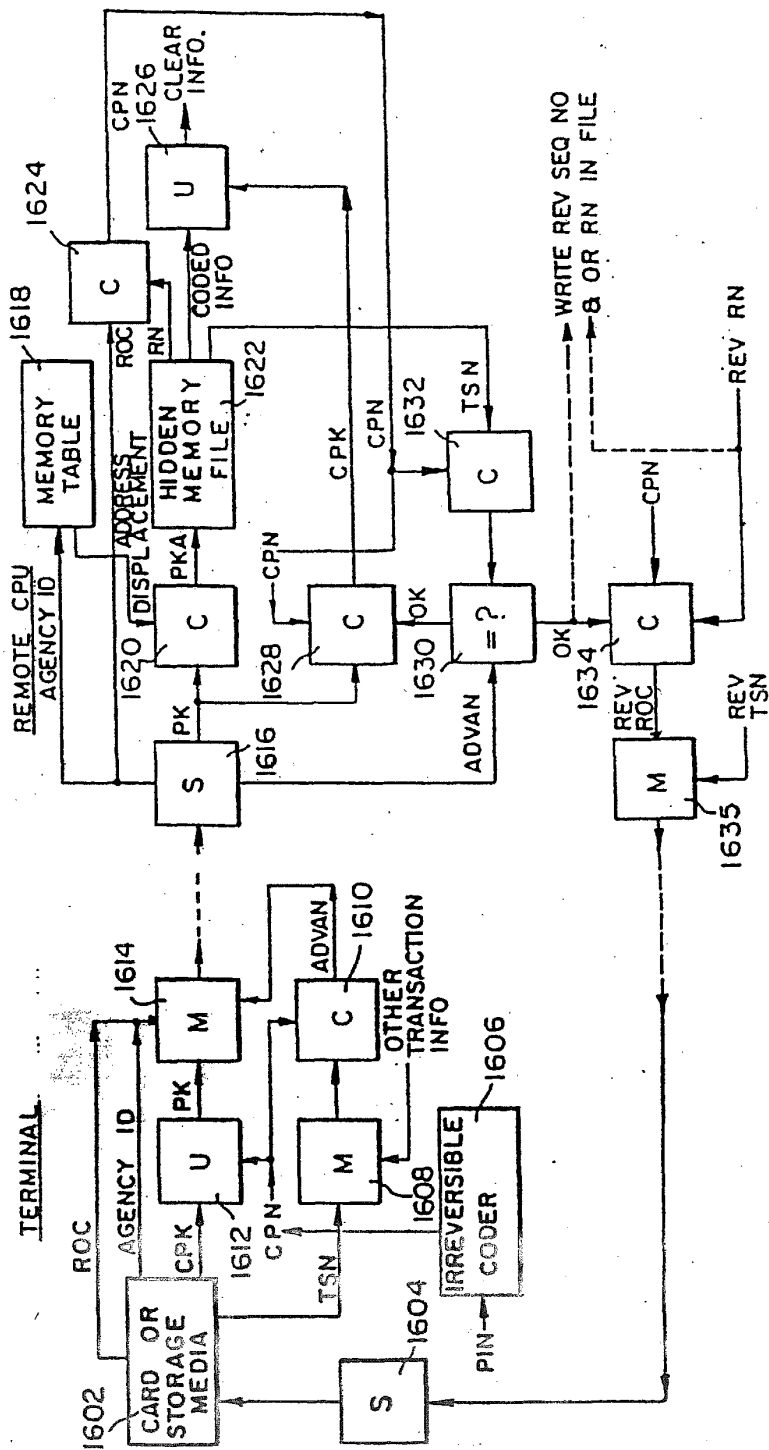


FIG. 16

872/16
116269

IN-440085



STAM0041620

FIG. 1

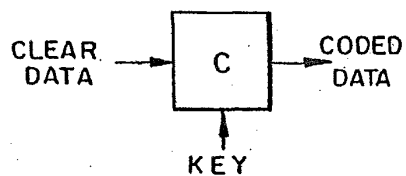


FIG. 2

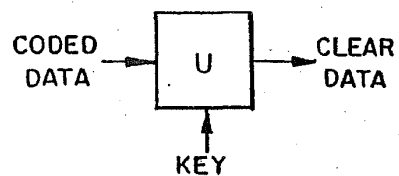


FIG. 3

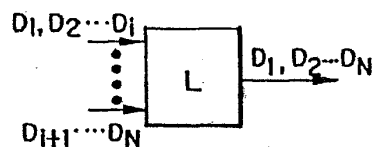


FIG. 4

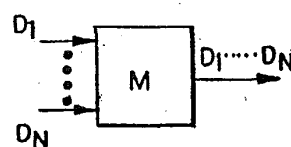


FIG. 5

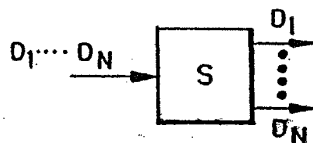
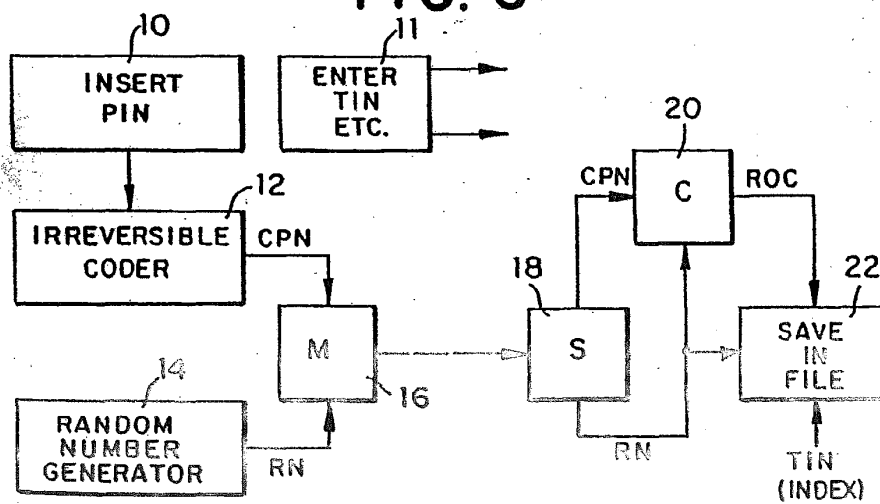


FIG. 6



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 1 OF 15



RECEIVED
DEC 21 1998
Group 2700

STAM0041622

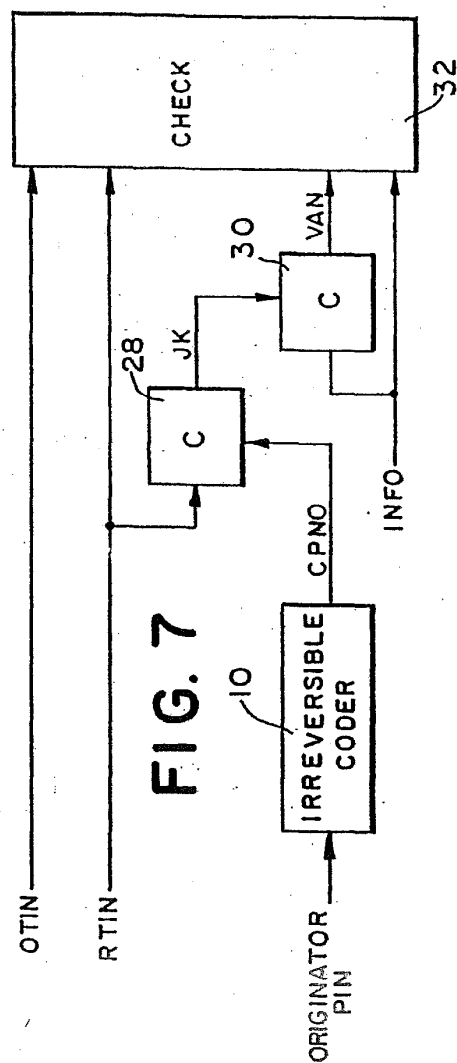


FIG. 7

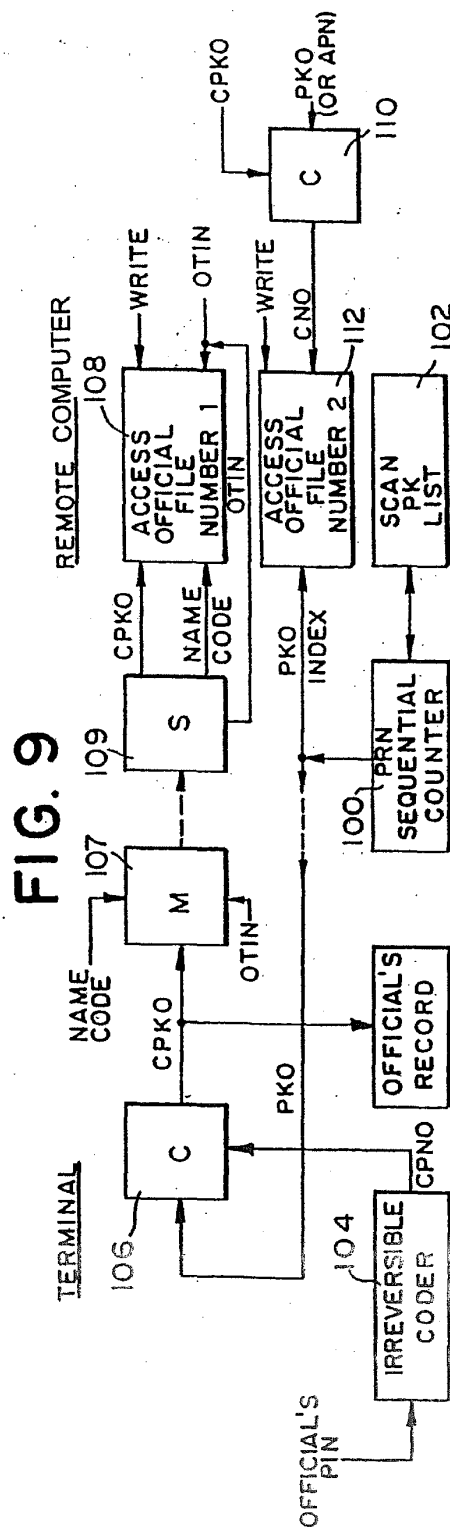


FIG. 9

PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 2 OF 15



RECEIVED

DEC 21 1998

Group 2700

STAM0041624

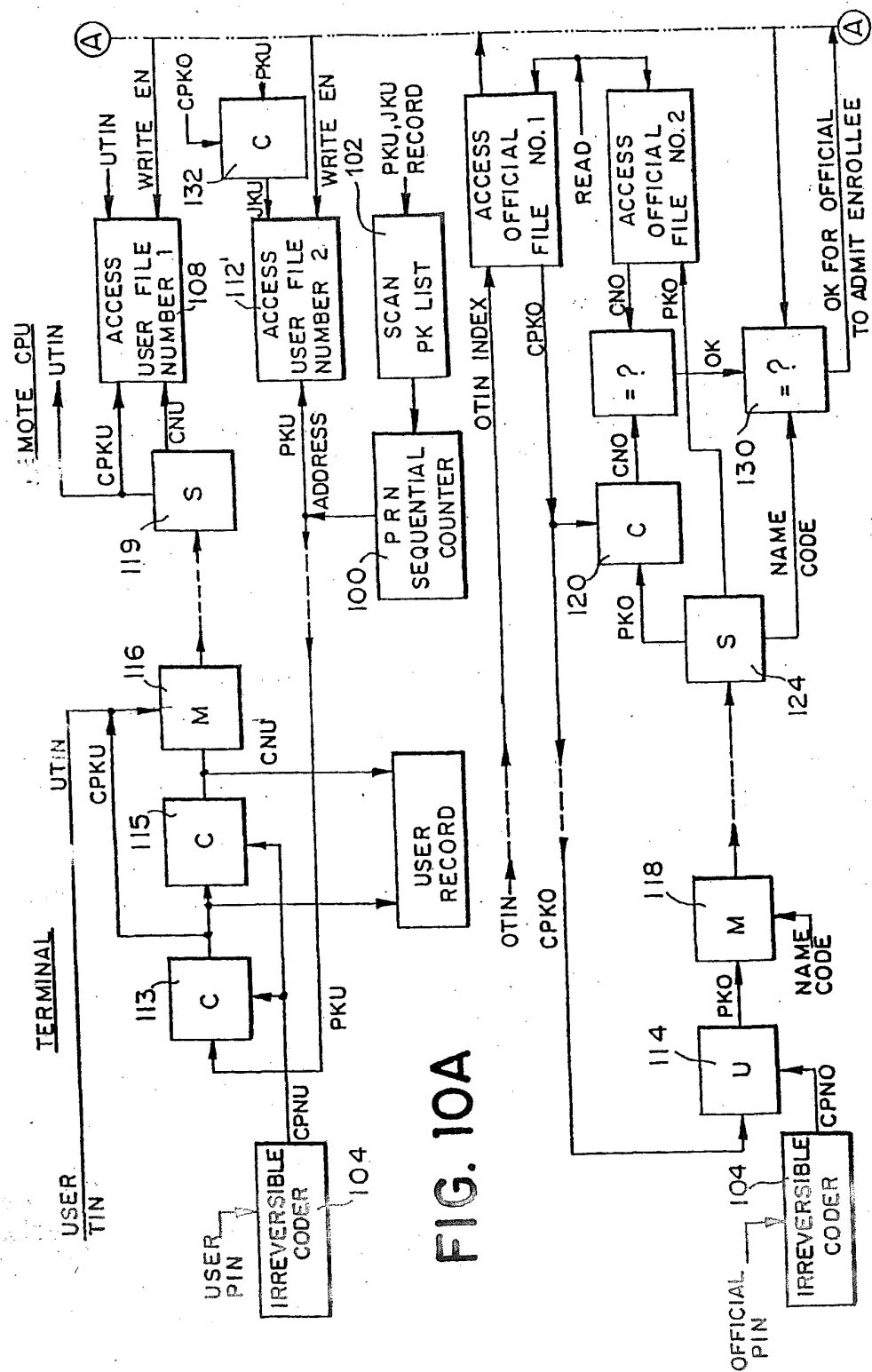


FIG. 10A

PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

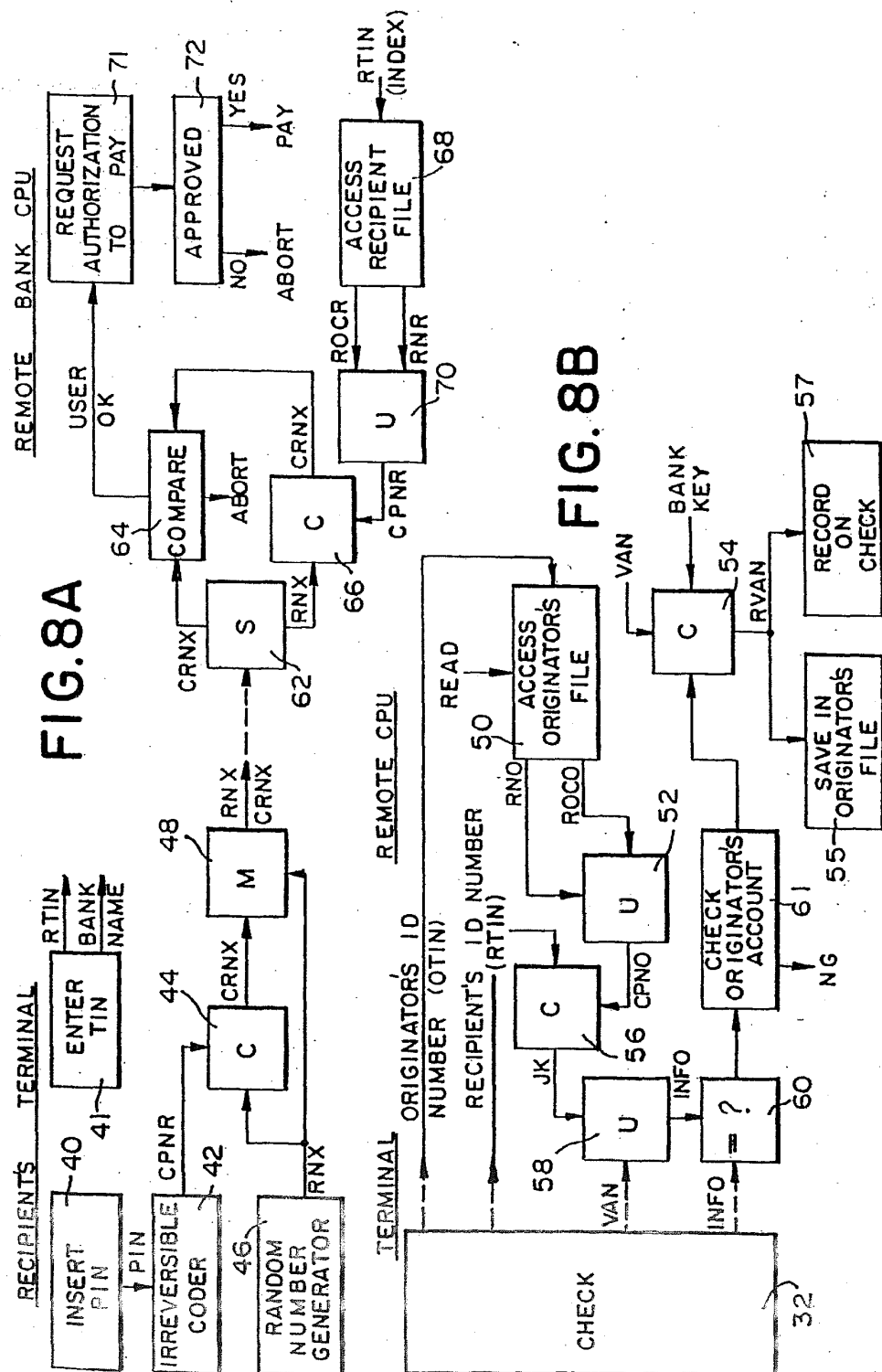
ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 4 OF 15



RECEIVED
DEC 21 1998
Group 2700

STAM0041626



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

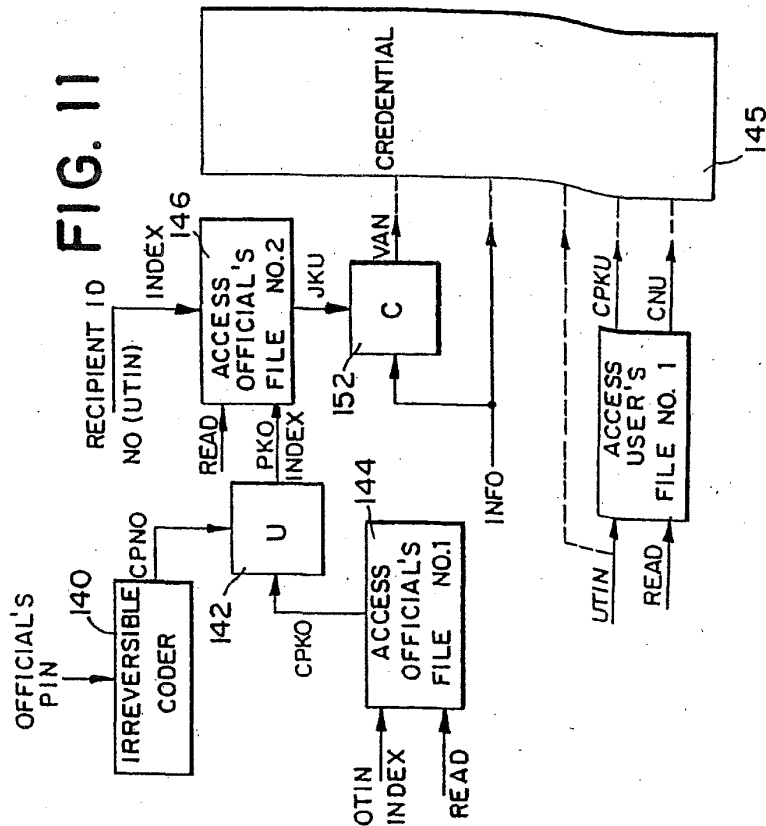
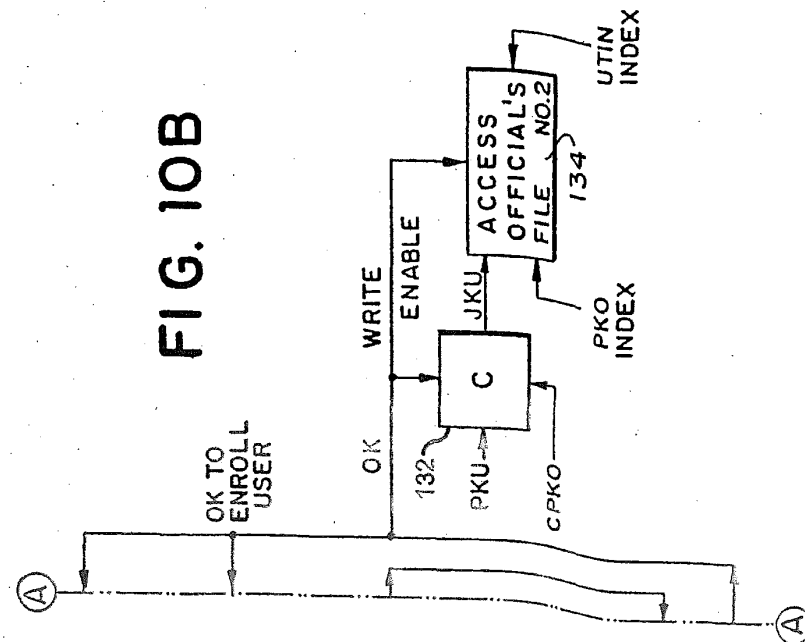
ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 3 OF 15



RECEIVED
DEC 21 1998
Group 2700

STAM0041628



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

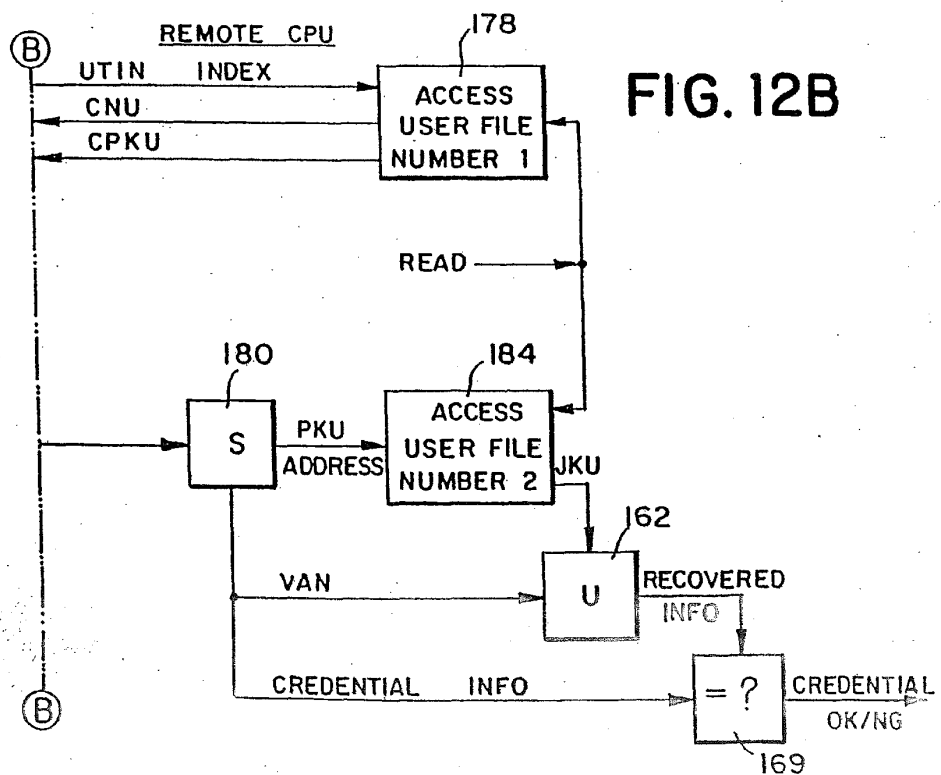
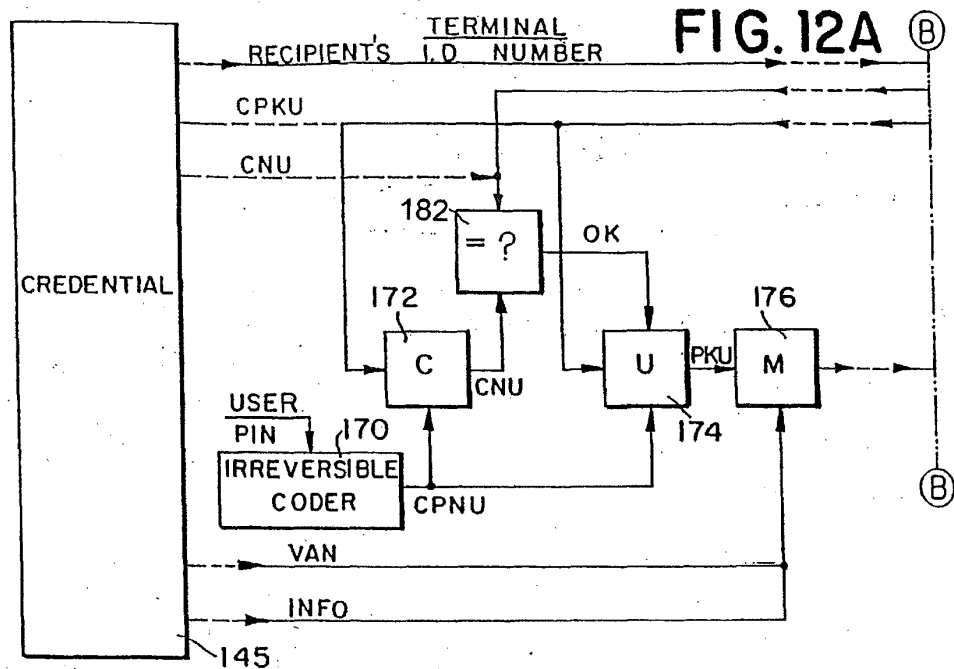
ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 5 OF 15



RECEIVED
DEC 1 1998
GPO 2700

STAM0041630



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPL. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

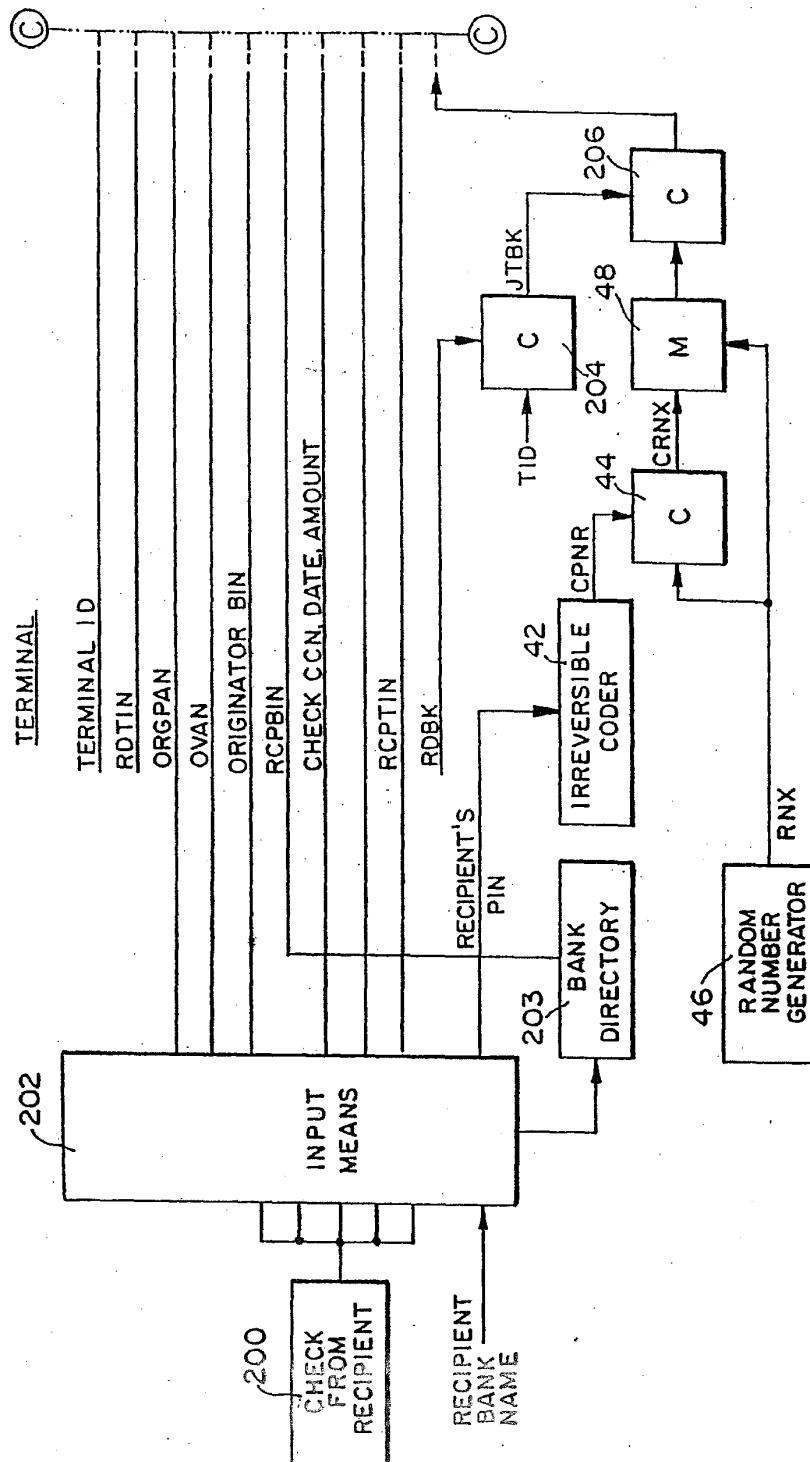
SHEET NO. 6 OF 15



RECEIVED
DEC 21 1998
Group 2/00

STAM0041632

FIG. 13A



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-IU7

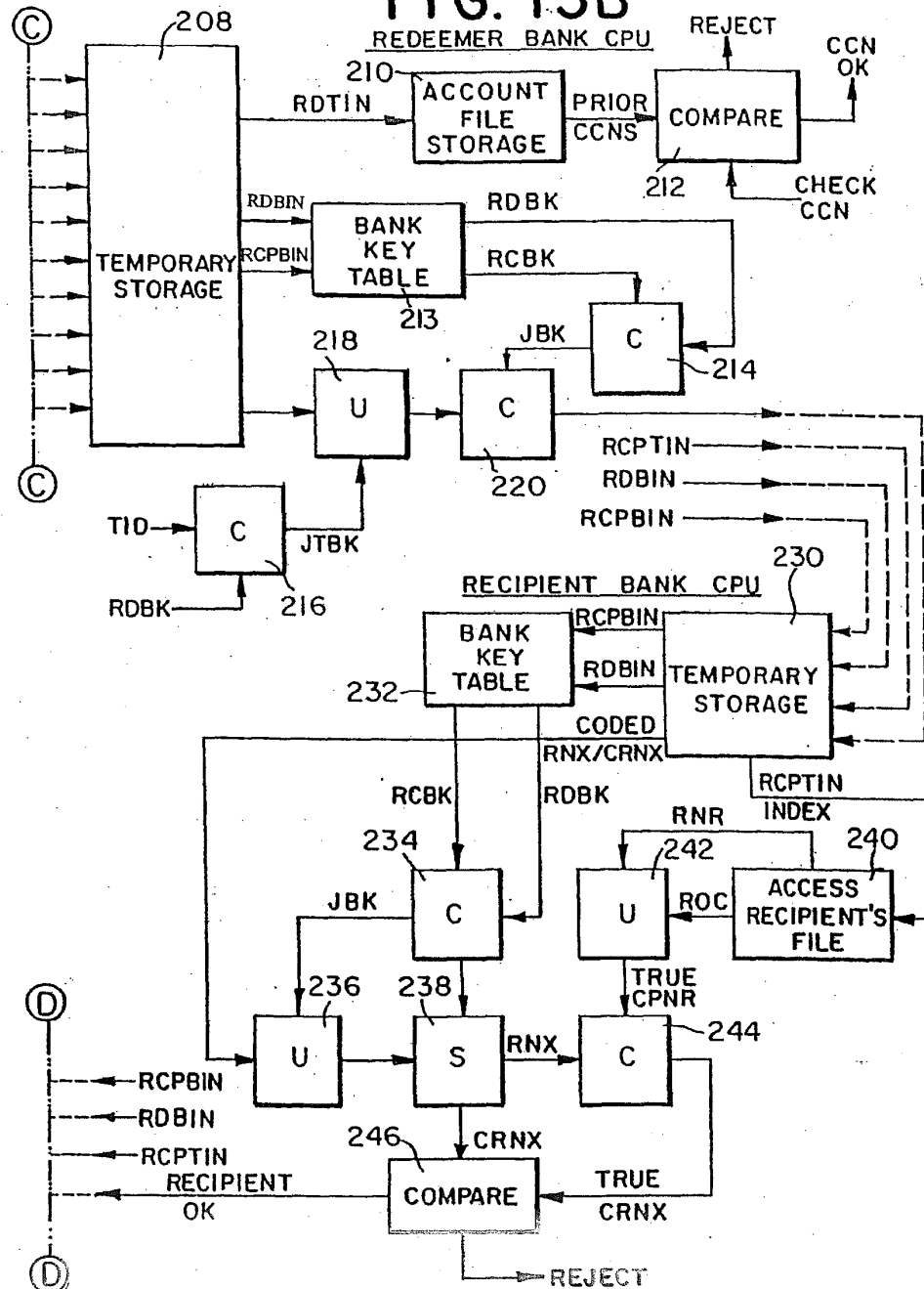
SHEET NO. 7 OF 15



RECEIVED
DEC 21 1998
GROUP 2700

STAM0041634

FIG. 13B



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

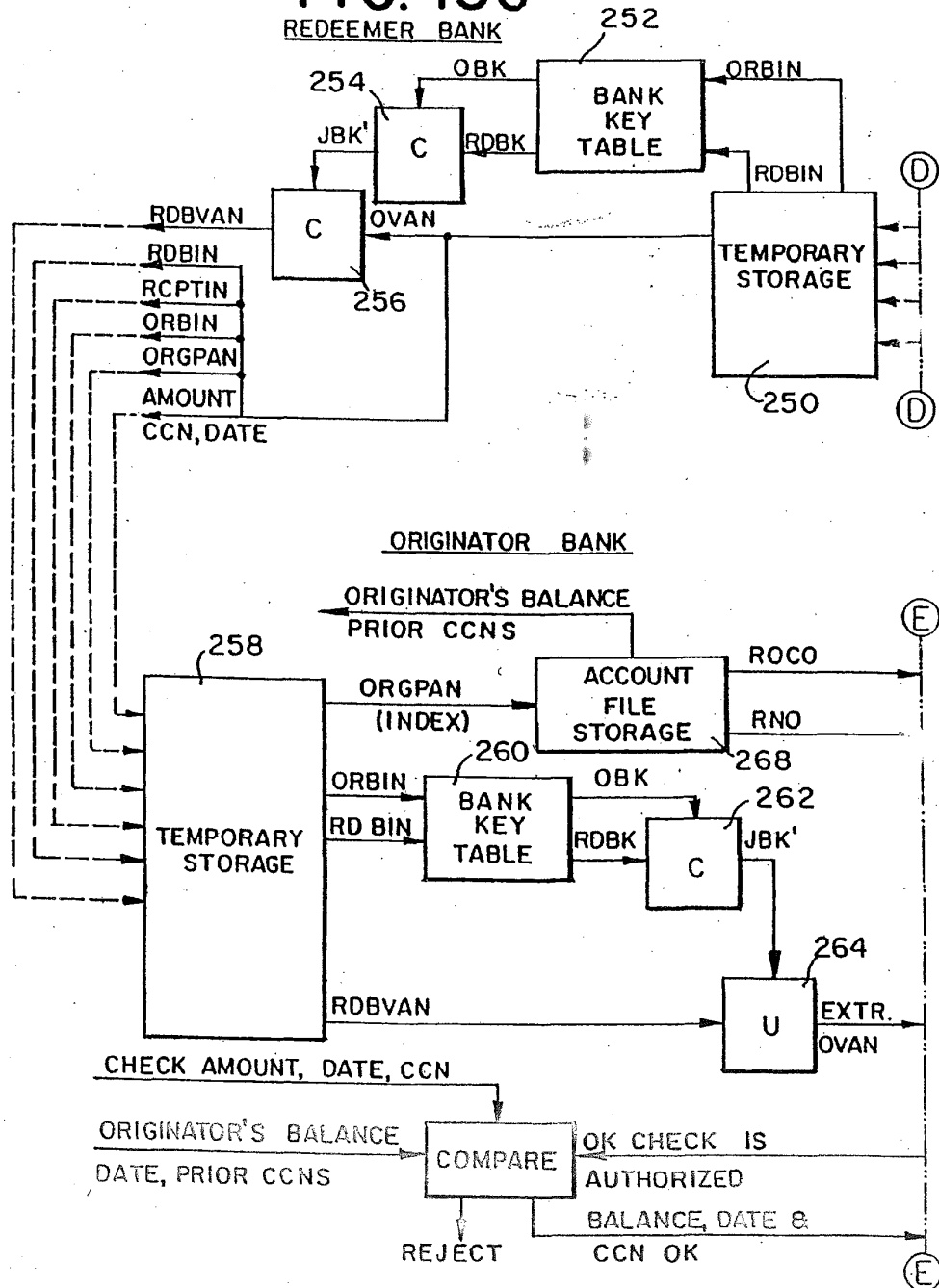
SHEET NO. 8 OF 15



RECEIVED
DEC 21 1998
Group 2700

STAM0041636

FIG. 13C



STAM0041637

PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

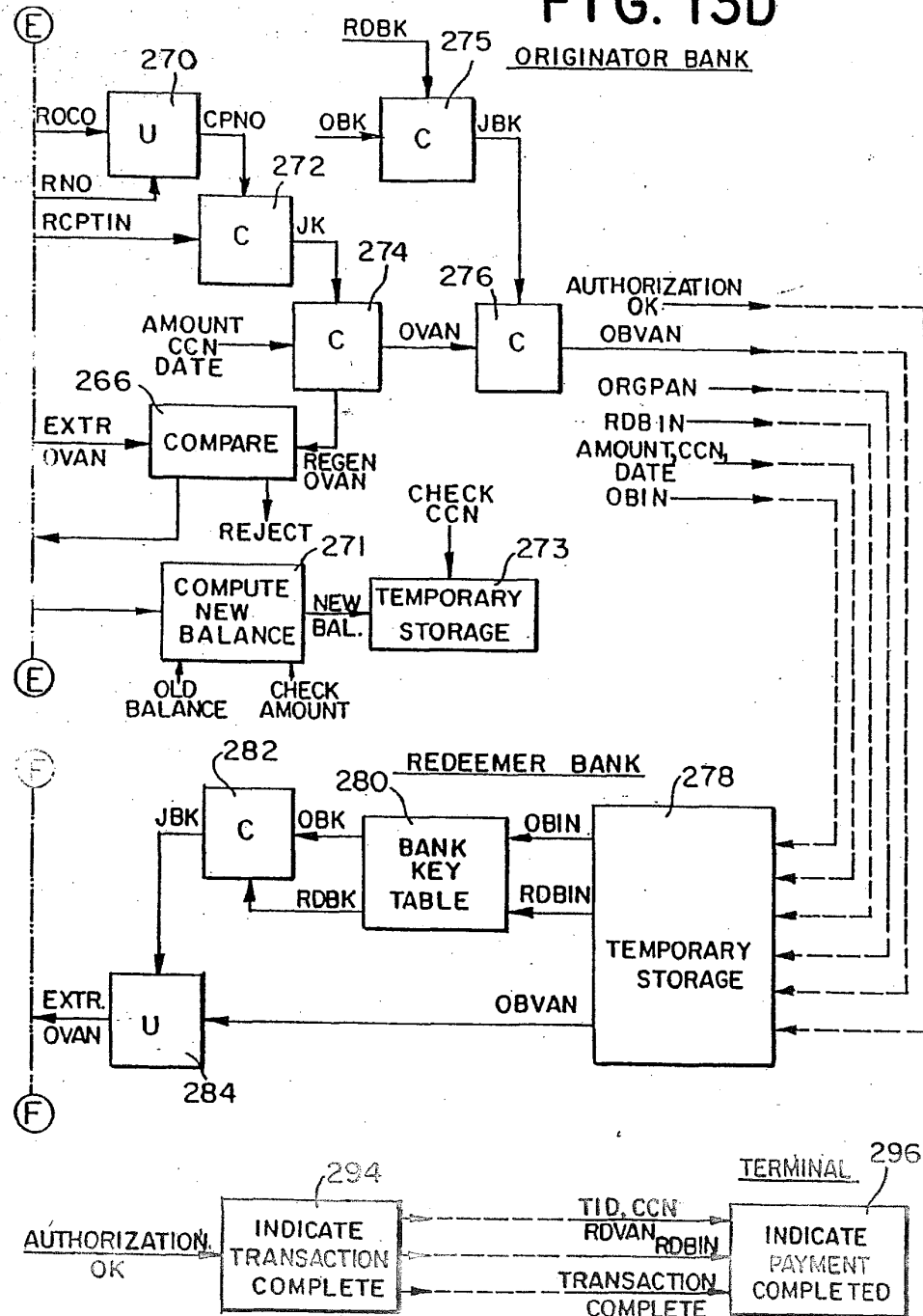
SHEET NO. 9 OF 15



RECEIVED
DEC 2-1 1998
Group 2700

STAM0041638

FIG. 13D





RECEIVED
DEC 21 1998
Group 2700

PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

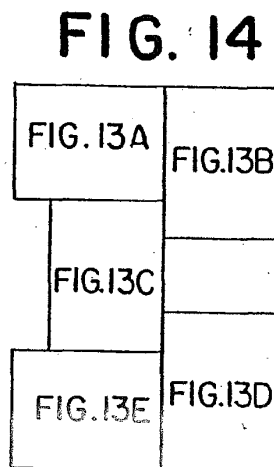
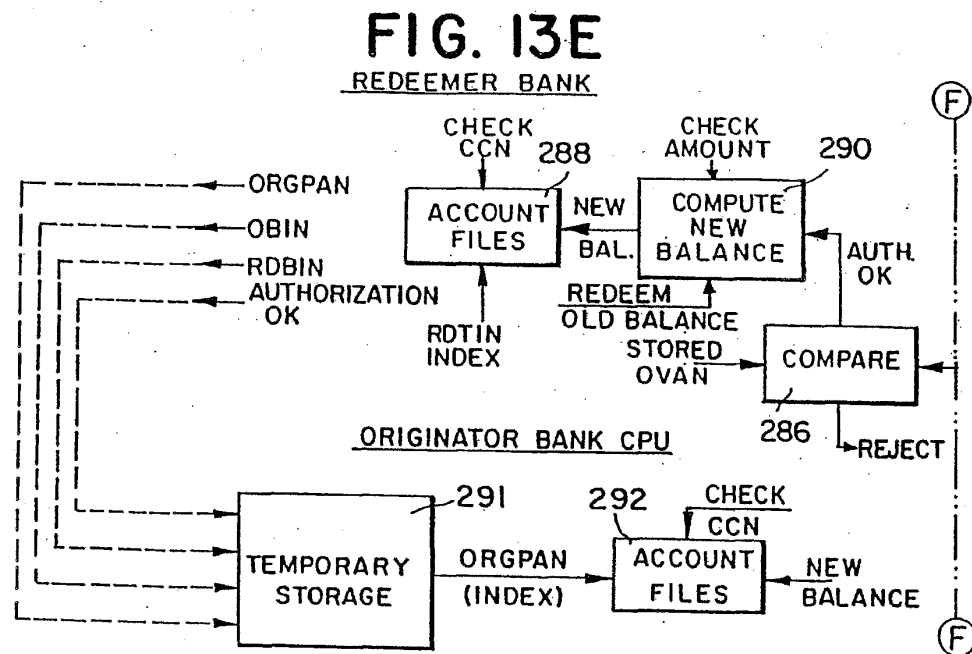
FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 10 OF 15

STAM0041640





RECEIVED
DEC 21 1998
Group 2700

PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 11 OF 15

STAM0041642

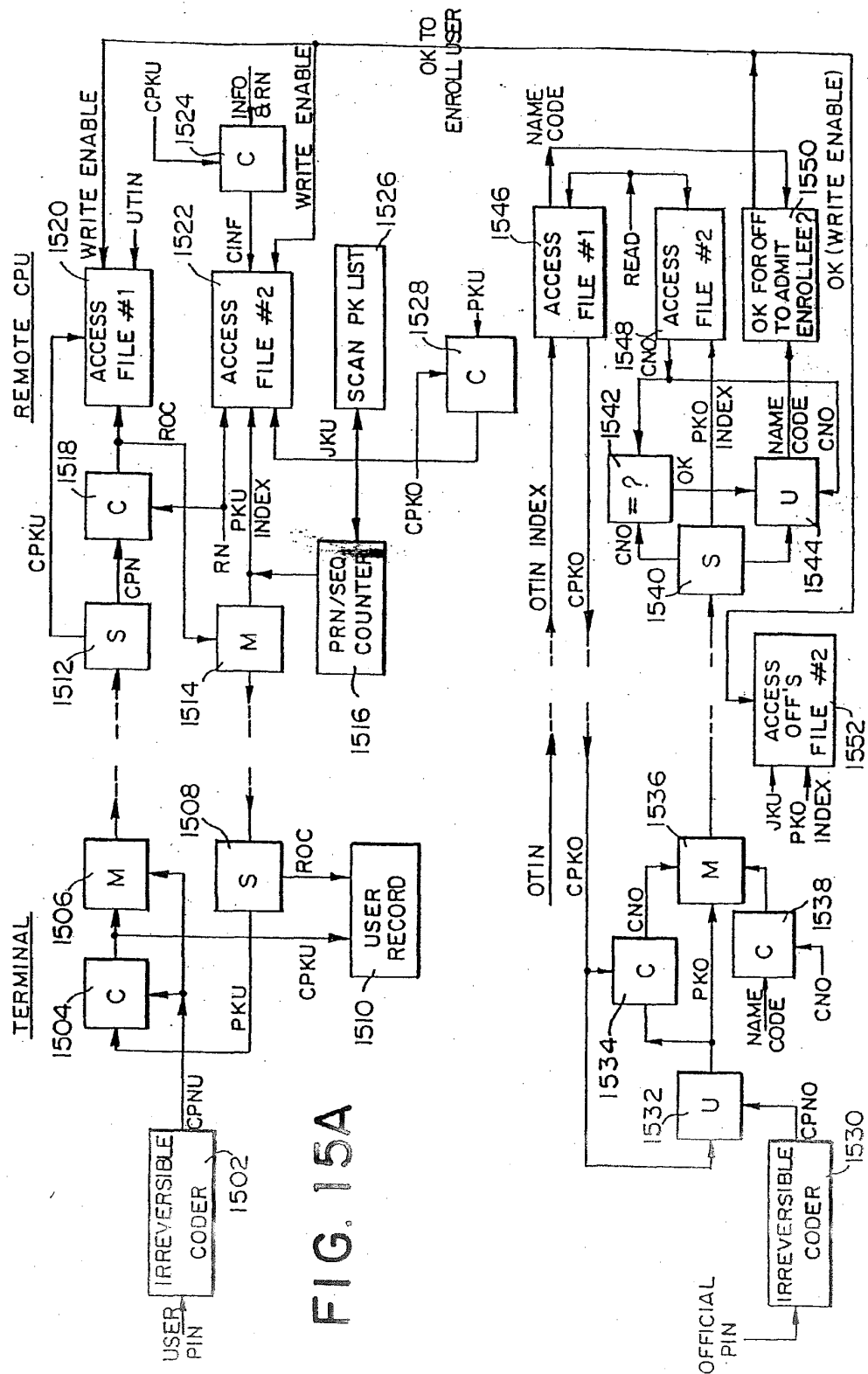


FIG. 15A

PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 12 OF 15



RECEIVED
DEC 21 1998
Group 2700

STAM0041644

CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL/COMPUTER

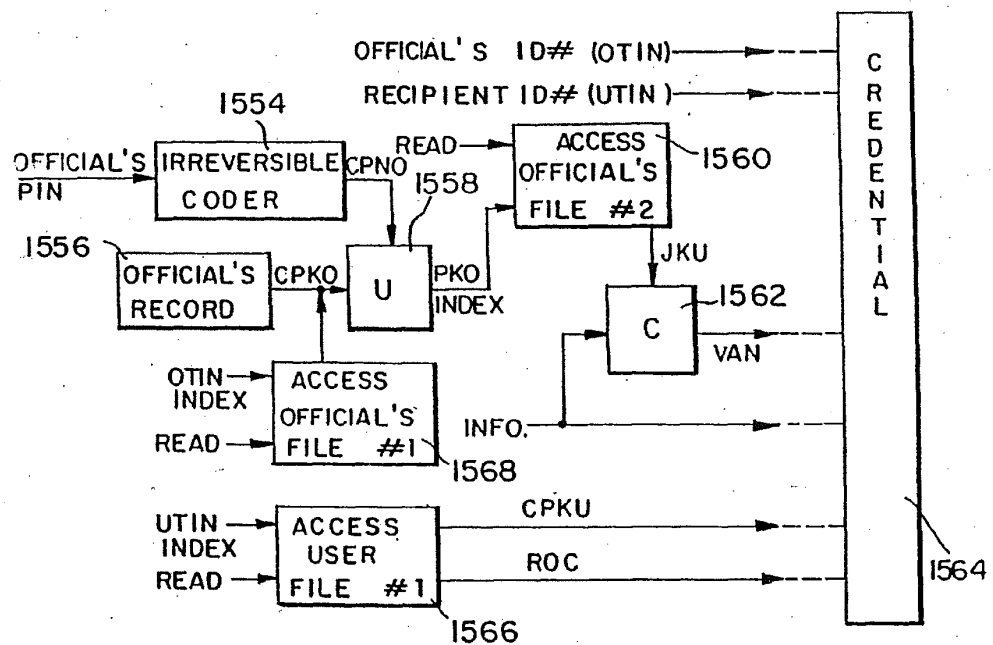


FIG. 15B



PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

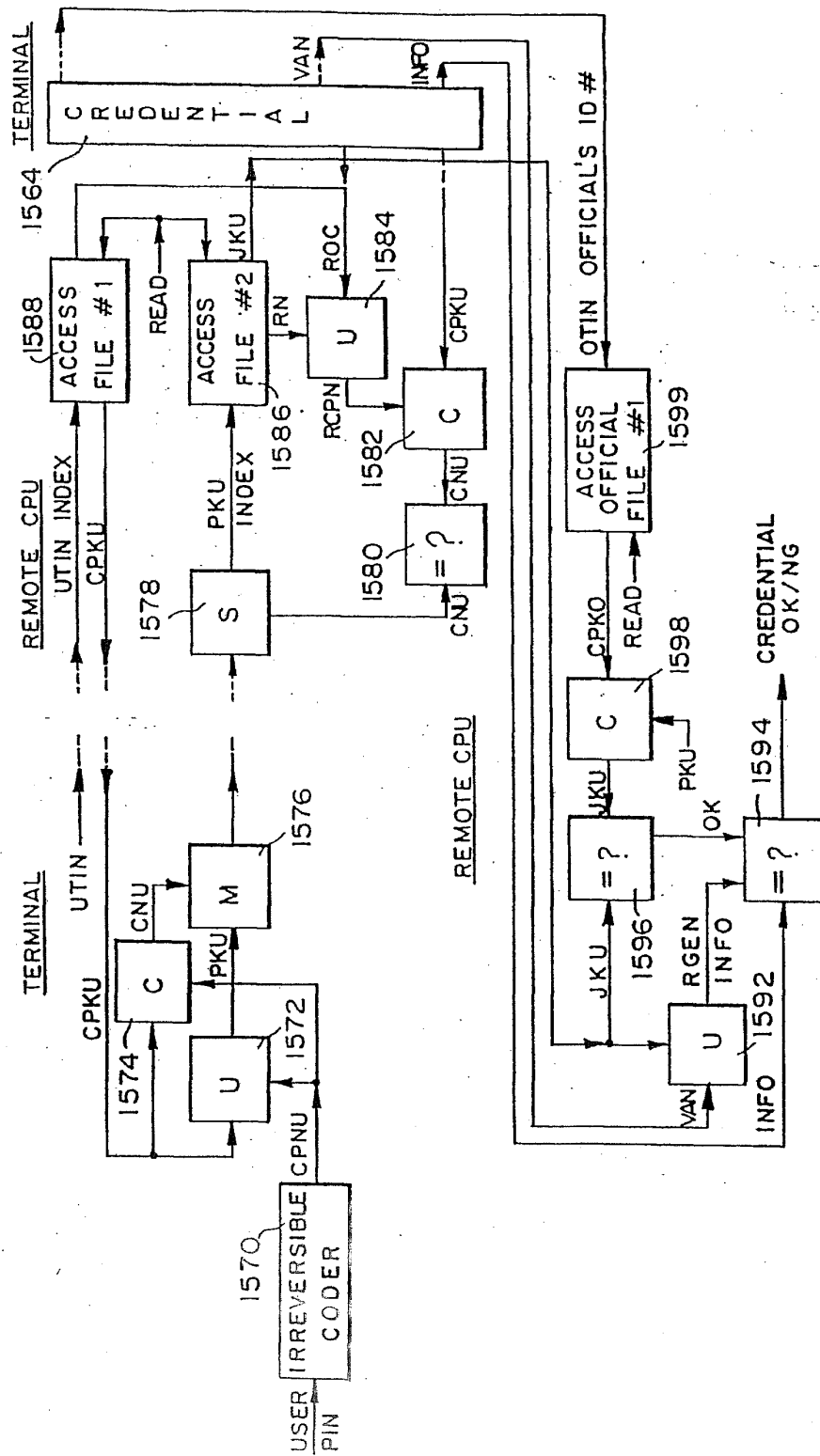
TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 13 OF 15

RECEIVED
DEC 21 1998
Group 2700

STAM0041646





RECEIVED
DEC 21 1998
Group 2700

PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 14 OF 15

STAM0041648

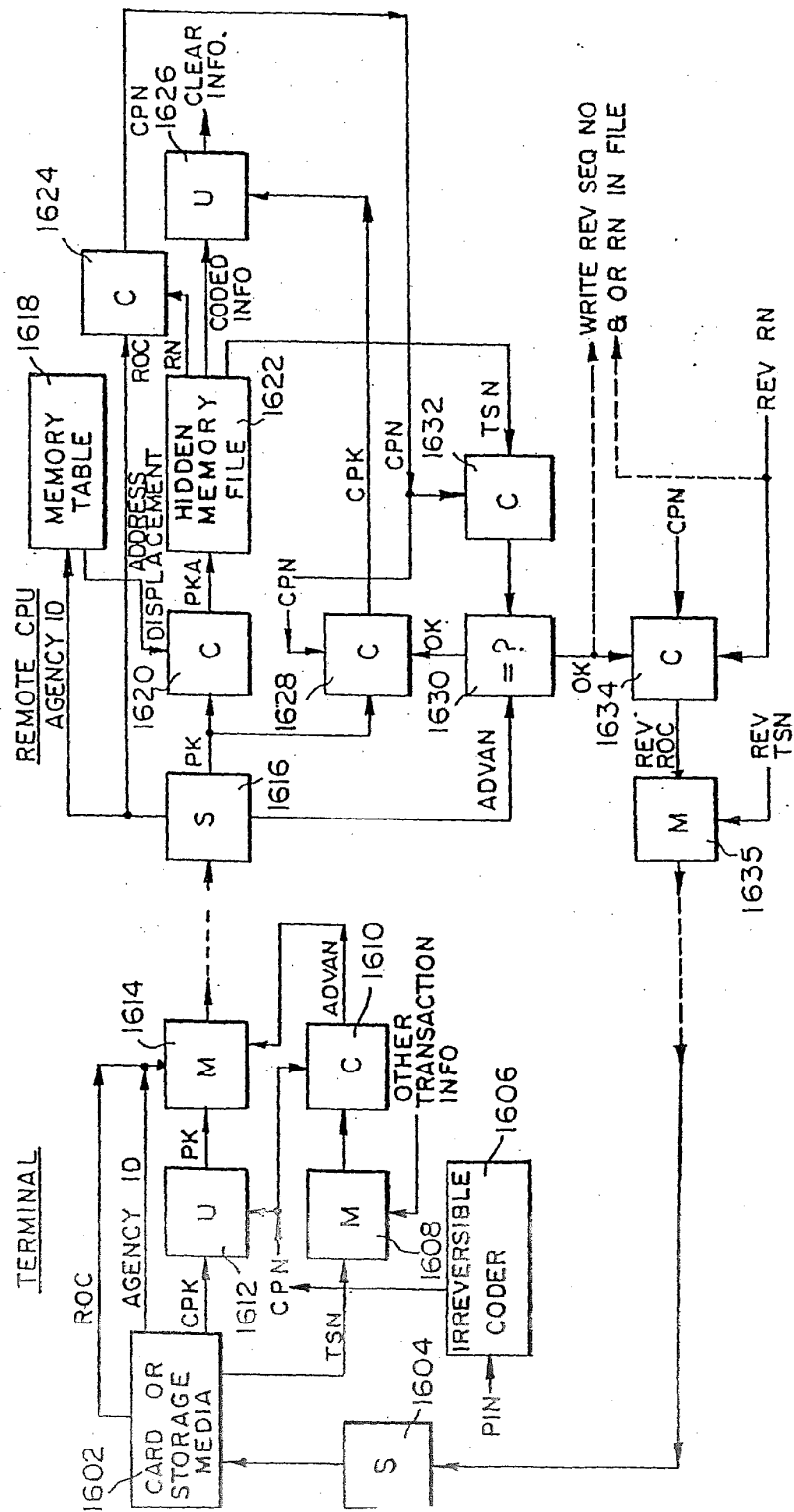


FIG. 16

STAM004164



RECEIVED
DEC 21 1998
Group 2700

PANITCH SCHWARZE JACOBS & NADEL, P.C.
INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

FILED: June 10, 1997

APPLN. NO.: 08/872,116

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 15 OF 15

STAM0041650



US005267314A

United States Patent [19]

[11] Patent Number: 5,267,314

Stambler

[45] Date of Patent: Nov. 30, 1993

[54] SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN

[76] Inventor: Leon Stambler, 7803 Boulder La., Parkland, Fla. 33067

[21] Appl. No.: 977,385

[22] Filed: Nov. 17, 1992

[51] Int. Cl.³ H04L 9/00

[52] U.S. Cl. 380/24; 380/4;

380/23; 380/25

[58] Field of Search 380/23, 24, 25, 4

[56] References Cited

U.S. PATENT DOCUMENTS

3,609,690	9/1971	Nissman	340/149 R
3,611,293	10/1971	Constable	340/149 A
3,657,521	4/1972	Constable	235/61.7 B
3,892,948	7/1975	Constable	340/149 R
3,938,091	2/1976	Atalla et al.	340/149 A
4,004,089	1/1977	Richard et al.	178/22
4,016,405	4/1977	McCune et al.	235/61.7 B
4,186,871	2/1980	Anderson et al.	235/380
4,198,619	4/1980	Atalla	340/149 A
4,208,575	6/1980	Haltof	235/380
4,223,403	9/1980	Konheim et al.	375/2
4,234,932	11/1980	Gorgens	364/900
4,264,782	4/1981	Konheim	178/22
4,268,715	5/1981	Atalla	178/22
4,281,215	7/1981	Atalla	178/22.08
4,283,599	8/1981	Atalla	178/22.1
4,302,810	11/1981	Bouricius et al.	380/24
4,304,990	12/1981	Atalla	235/380
4,317,957	3/1982	Sendrow	178/22.08
4,319,079	3/1982	Best	380/4
4,328,414	5/1982	Atalla	235/380
4,386,266	5/1983	Chesarek	235/380
4,498,000	2/1985	Decavele et al.	235/380
4,590,470	5/1986	Koenig	340/825.31
4,605,820	8/1986	Campbell, Jr.	380/24
4,665,396	5/1987	Dieleman	380/23
4,686,357	8/1987	Douno et al.	235/379

4,720,859	1/1988	Aaro et al.	380/23
4,734,858	3/1988	Schlaflly	364/408
4,755,940	7/1988	Bracht et al.	364/408
4,797,920	1/1989	Stein	380/24
4,799,061	1/1989	Abraham et al.	340/825.34
4,908,861	3/1990	Bracht et al.	380/25
4,928,098	5/1990	Dannhaeuser	340/825.56
4,933,969	6/1990	Marshall et al.	380/125
4,935,962	6/1990	Austin	380/25
4,947,028	8/1990	Gorog	235/381
4,965,568	10/1990	Atalla et al.	380/24
4,977,595	12/1990	Ohta et al.	380/24
4,992,783	2/1991	Zdunek et al.	340/825.340
5,016,274	5/1991	Micali et al.	380/23
5,023,908	6/1991	Weiss	380/23
5,163,098	11/1992	Dahbura	380/24

Primary Examiner—Salvatore Cangialosi

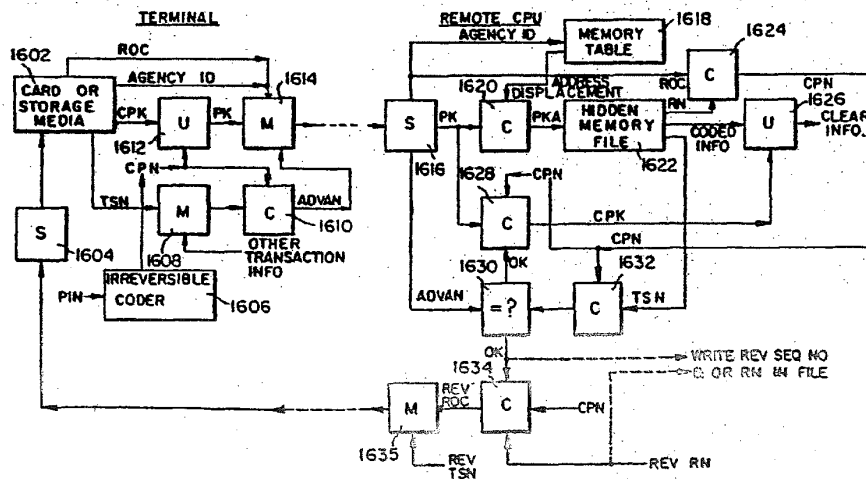
Attorney, Agent, or Firm—Panitch Schwarze Jacobs & Nadel

[57]

ABSTRACT

A transaction system is disclosed wherein, when a transaction, document or thing needs to be authenticated, information associated with one or more of the parties involved is coded together to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information.

22 Claims, 15 Drawing Sheets



STAM0041651

FIG. 1

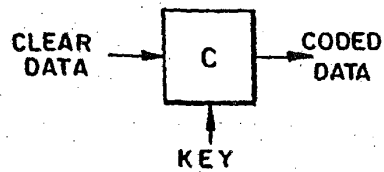


FIG. 2

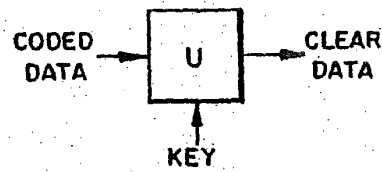


FIG. 3

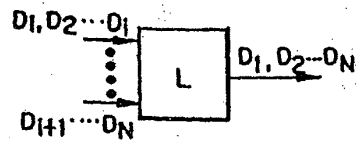


FIG. 4

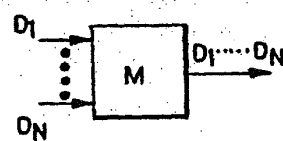


FIG. 5

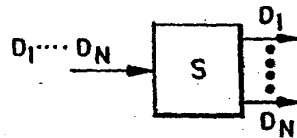
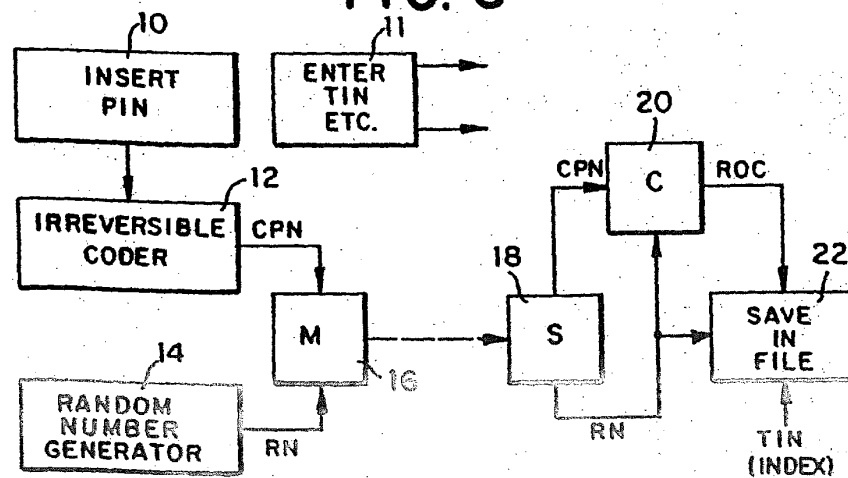
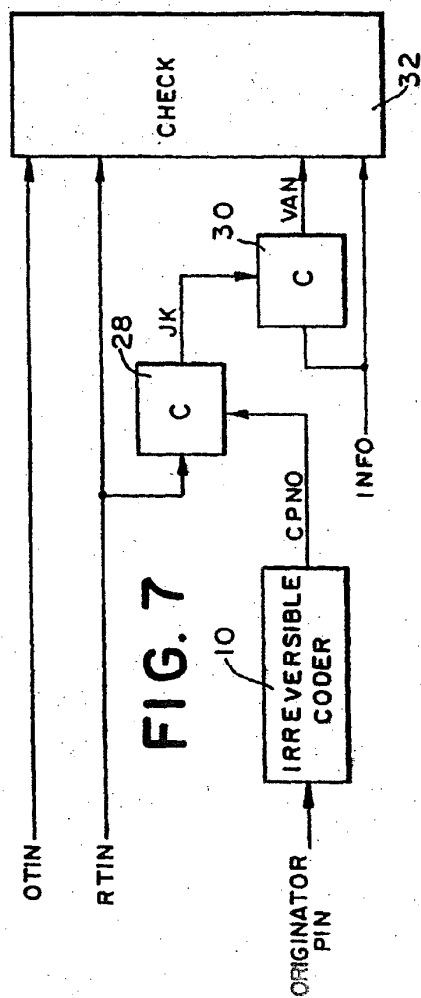
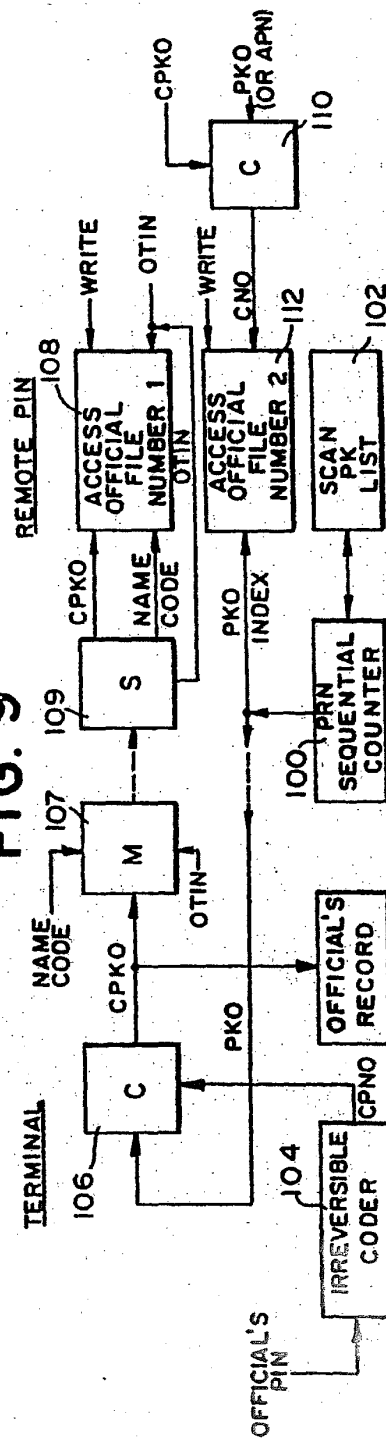


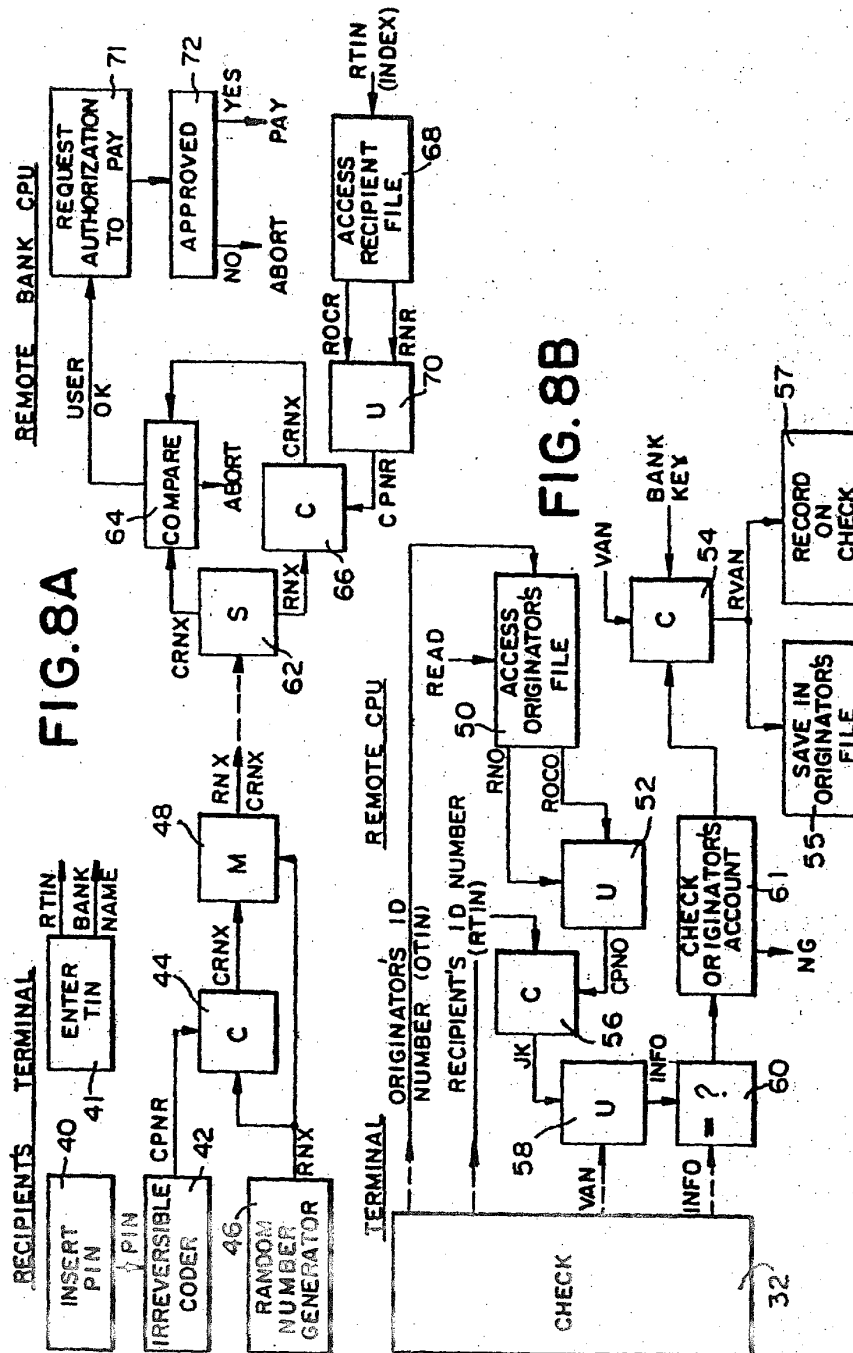
FIG. 6

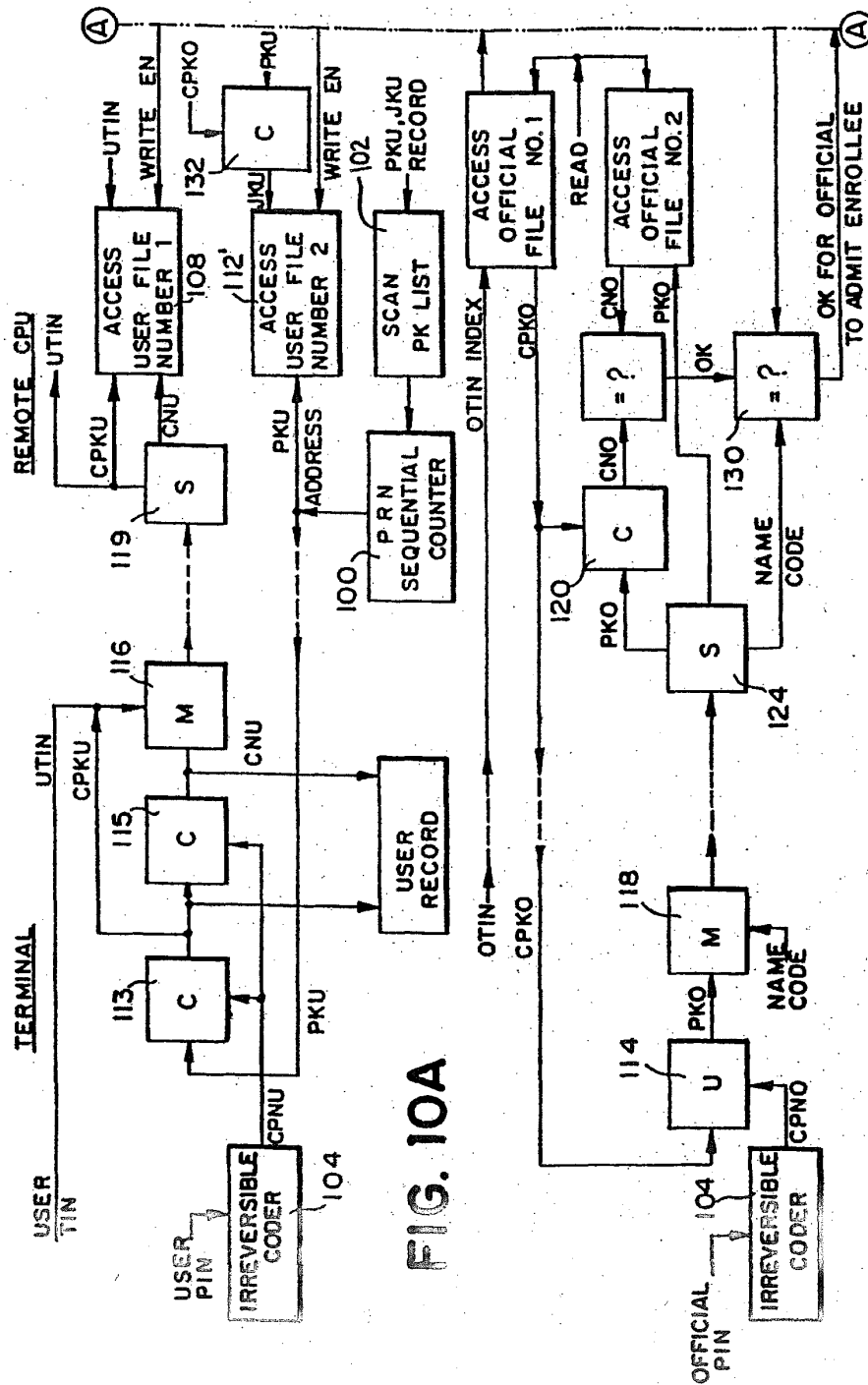


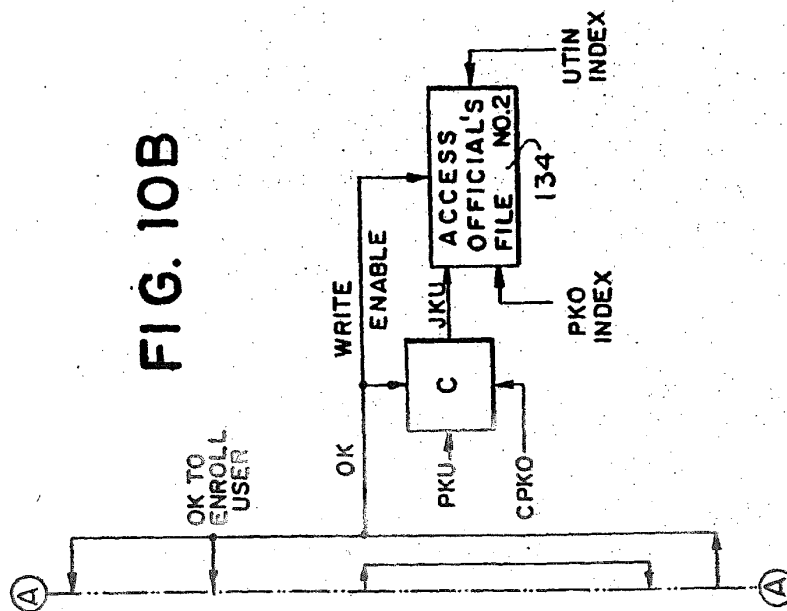
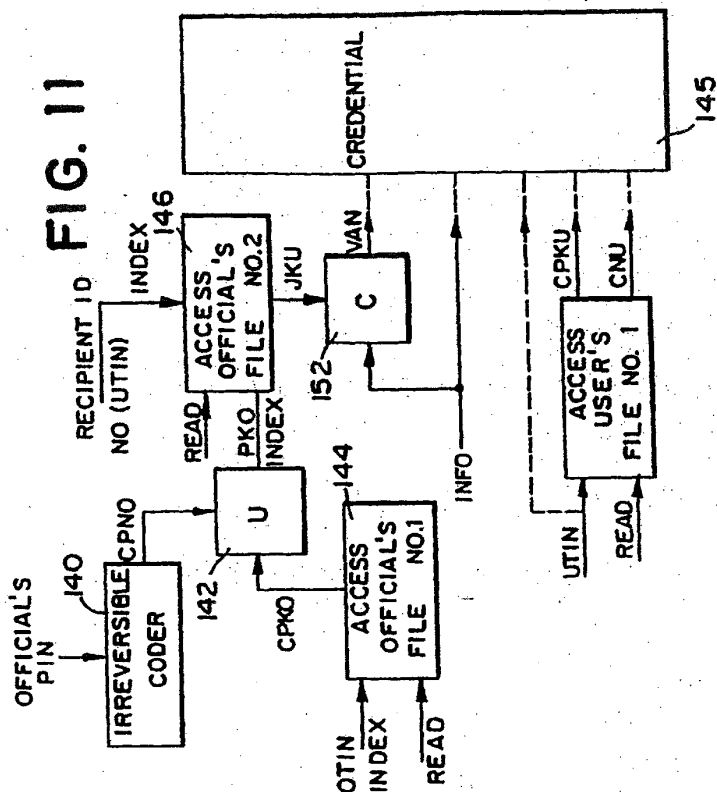


தெ









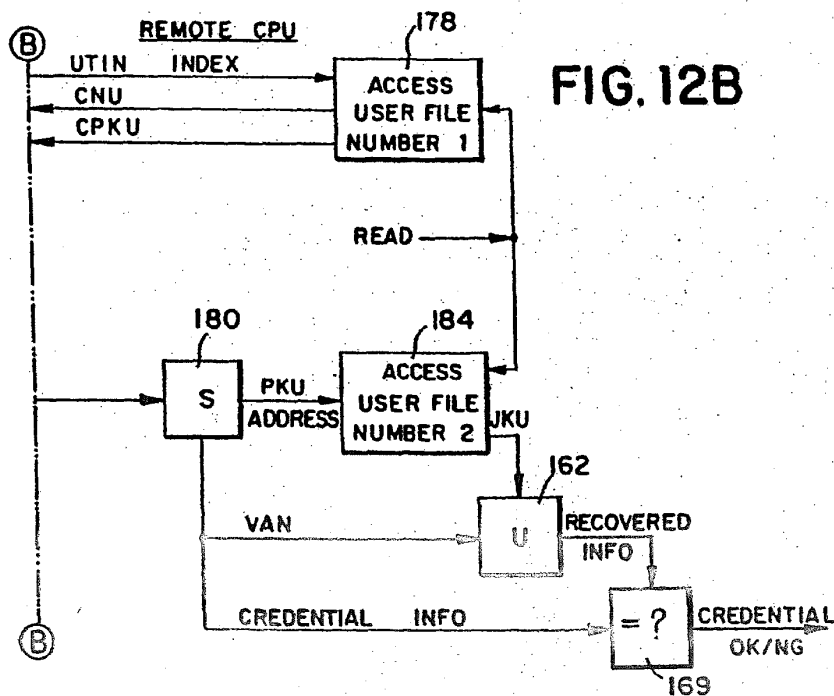
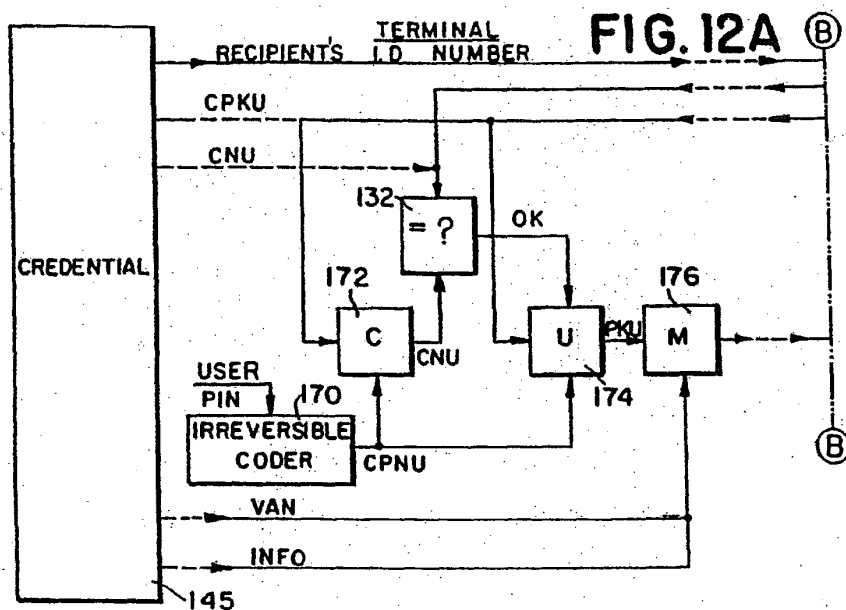
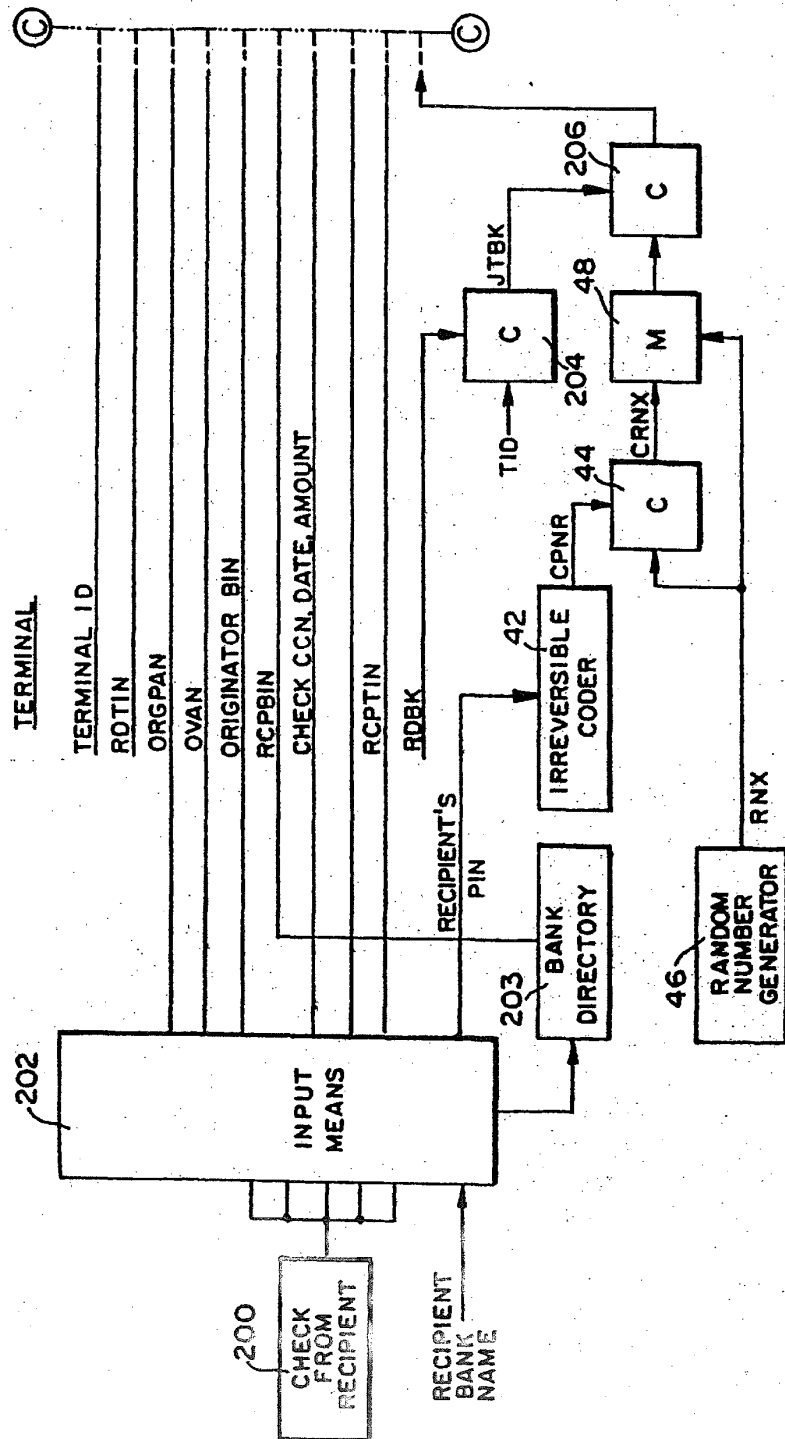


FIG. 13A



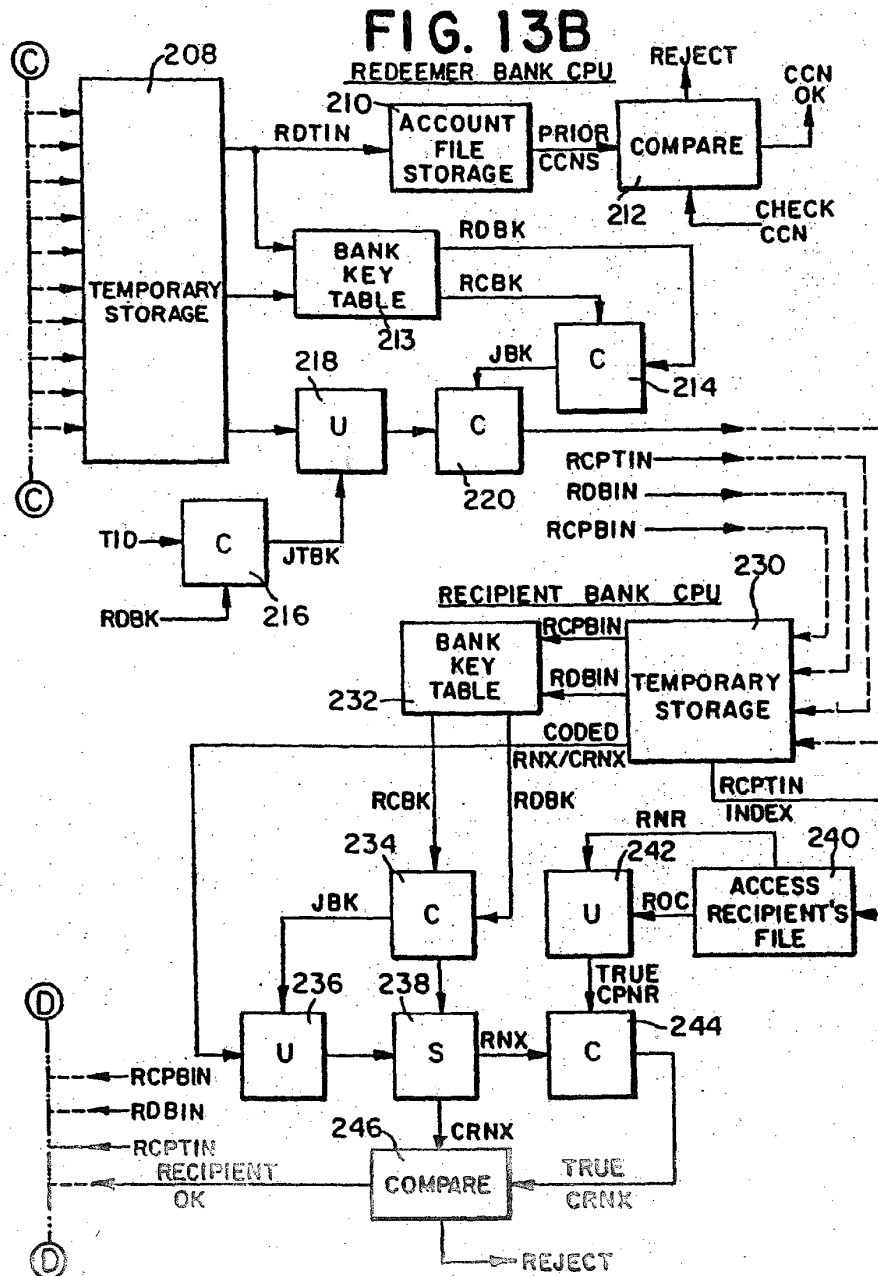


FIG. 13C

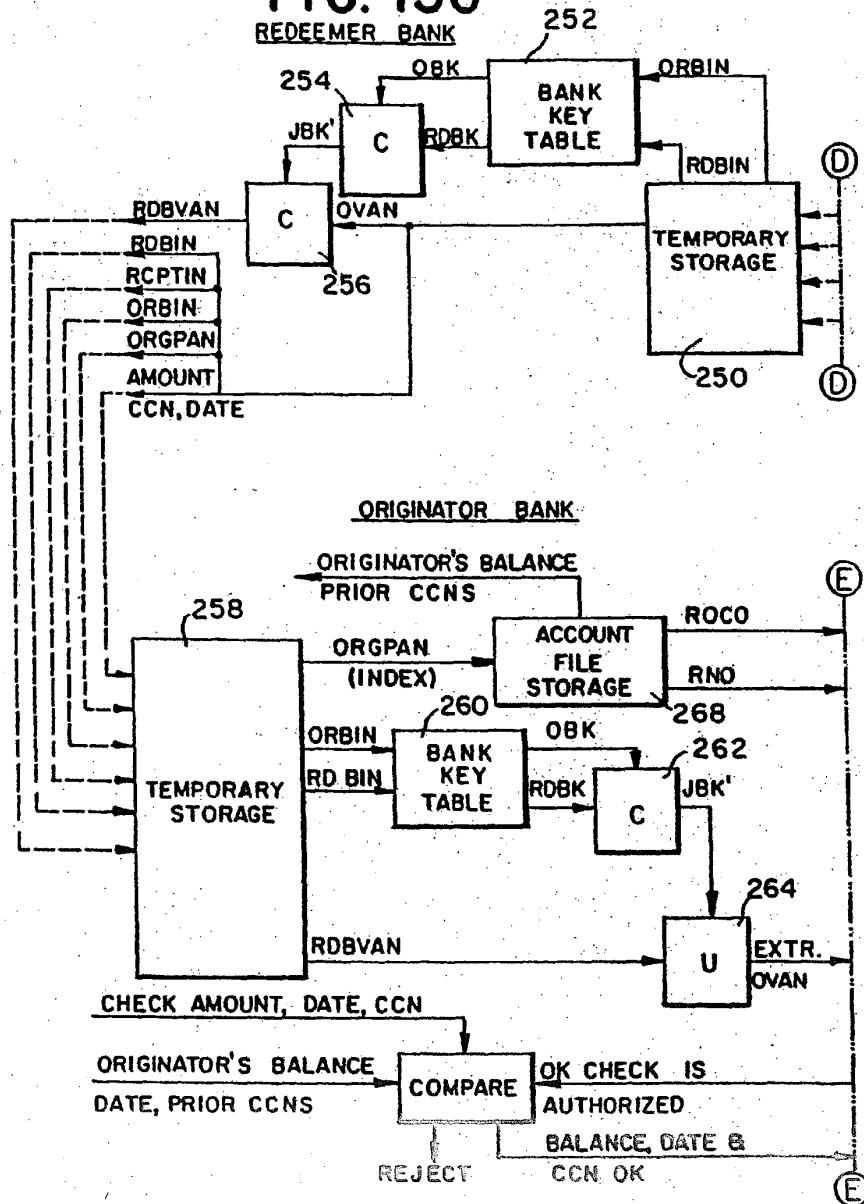
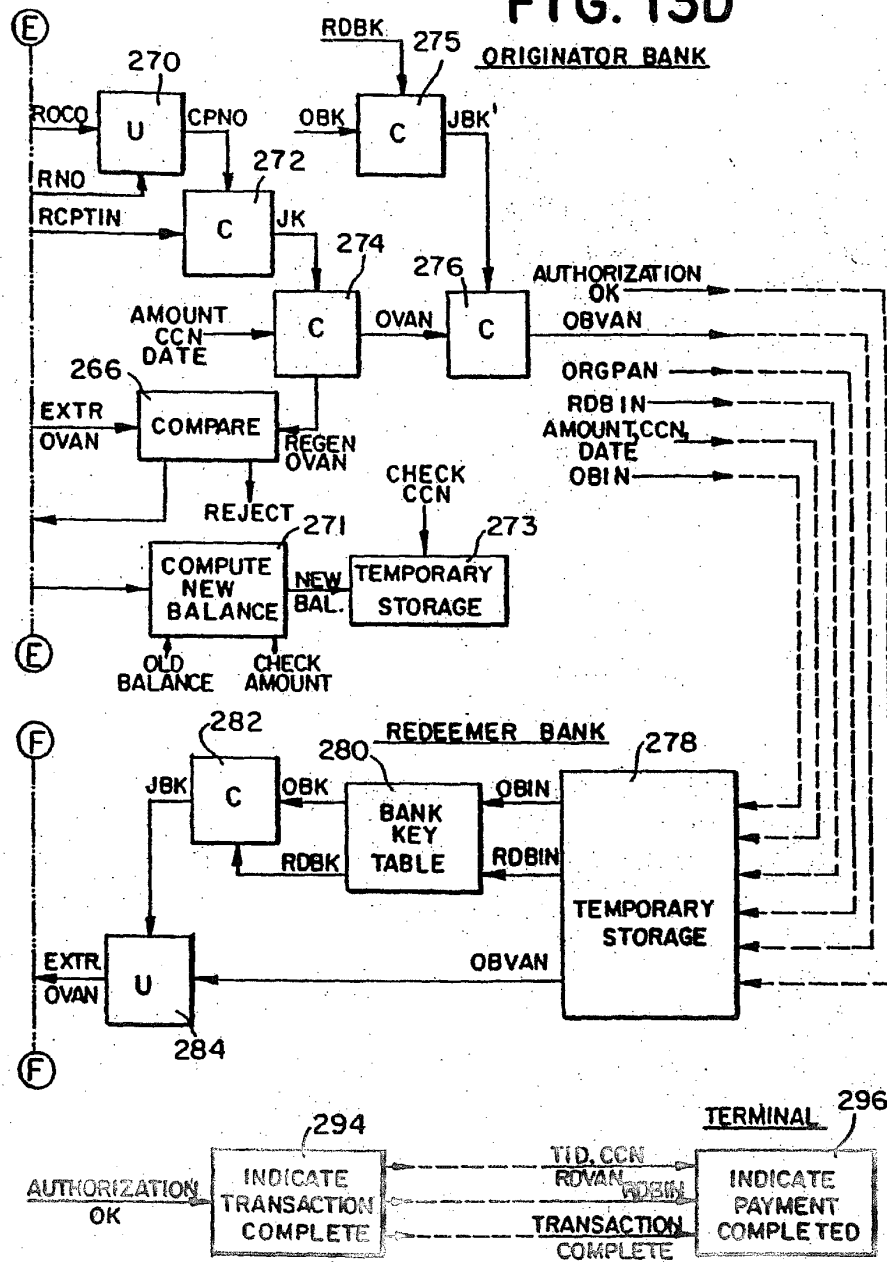
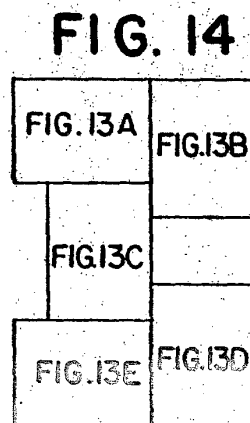
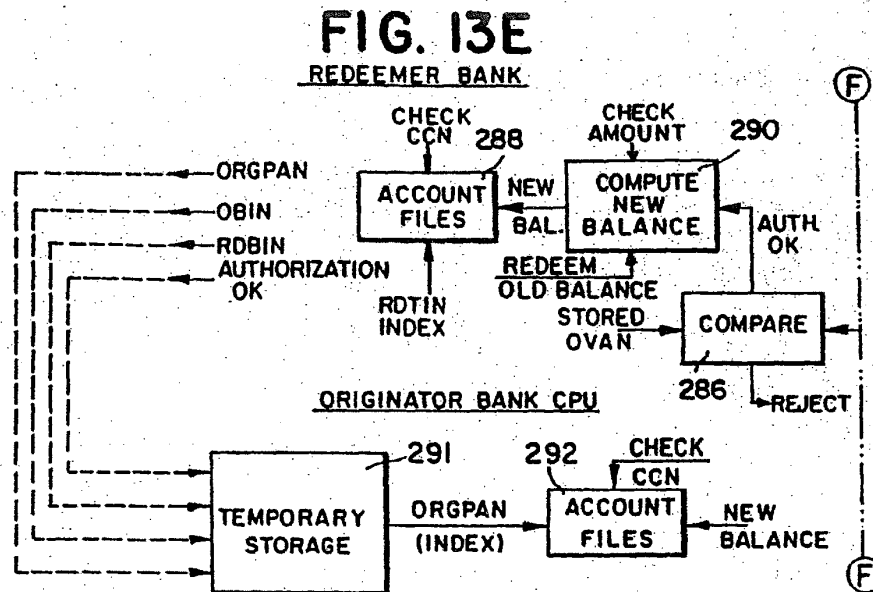
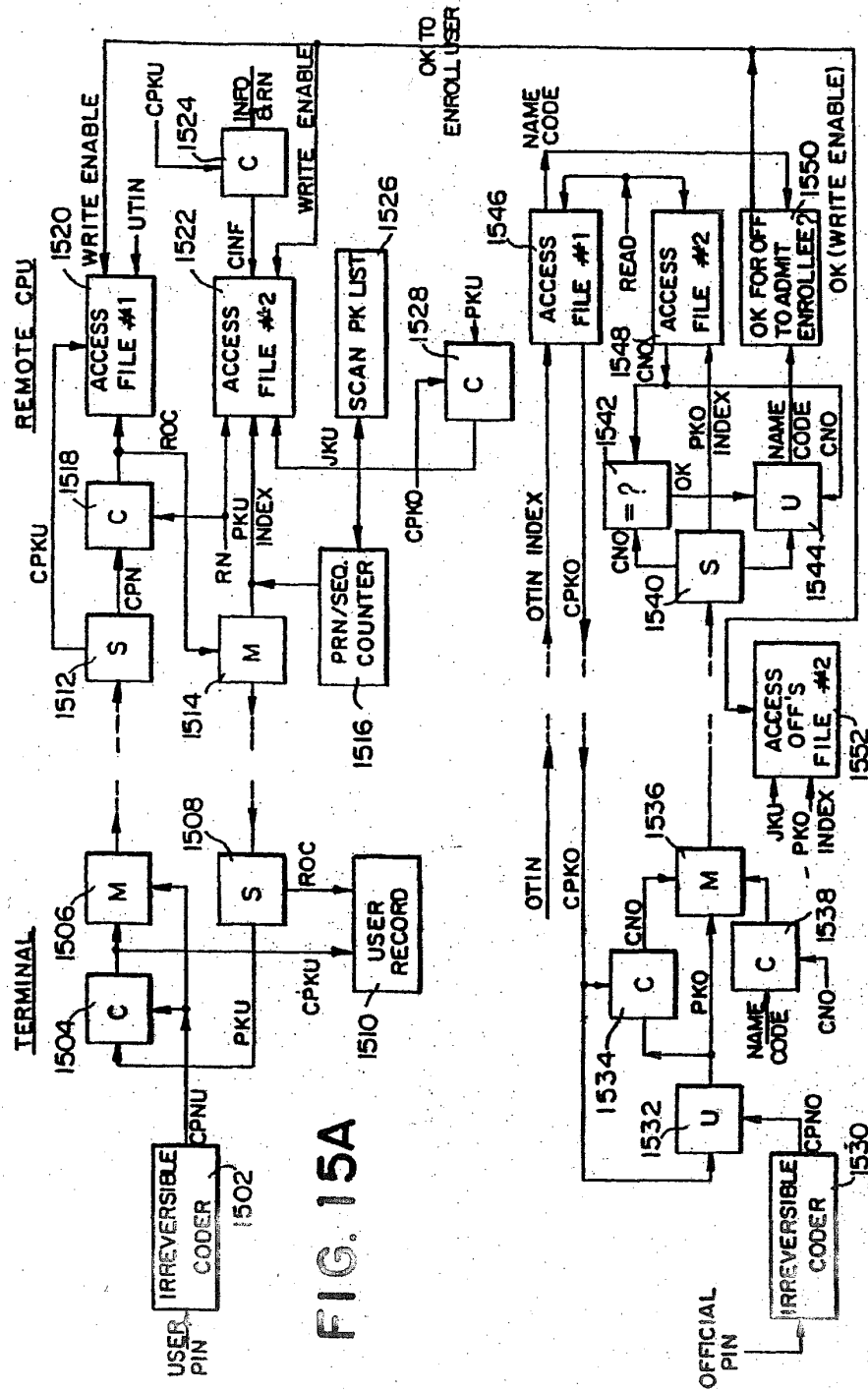


FIG. 13D



STAM0041661





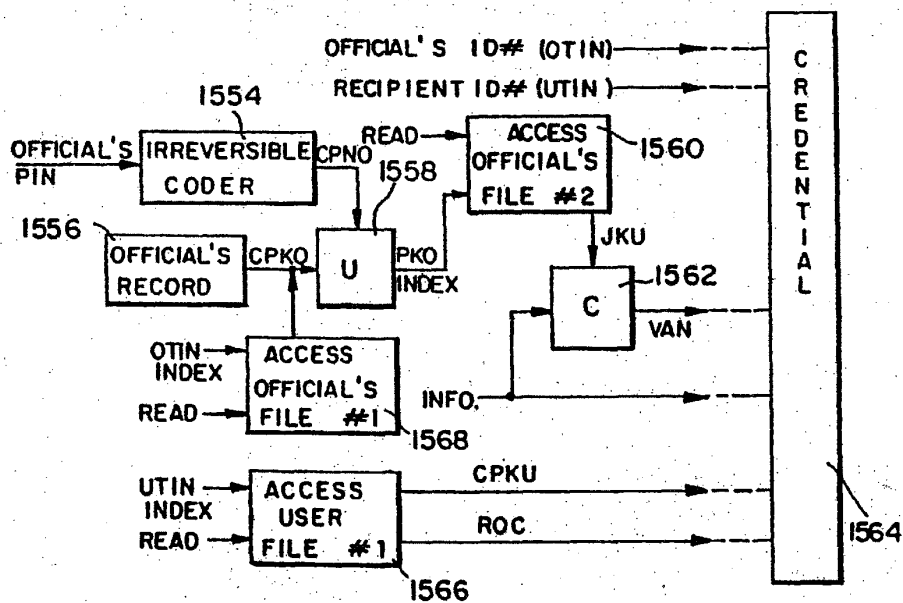
CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL/COMPUTER

FIG. 15B

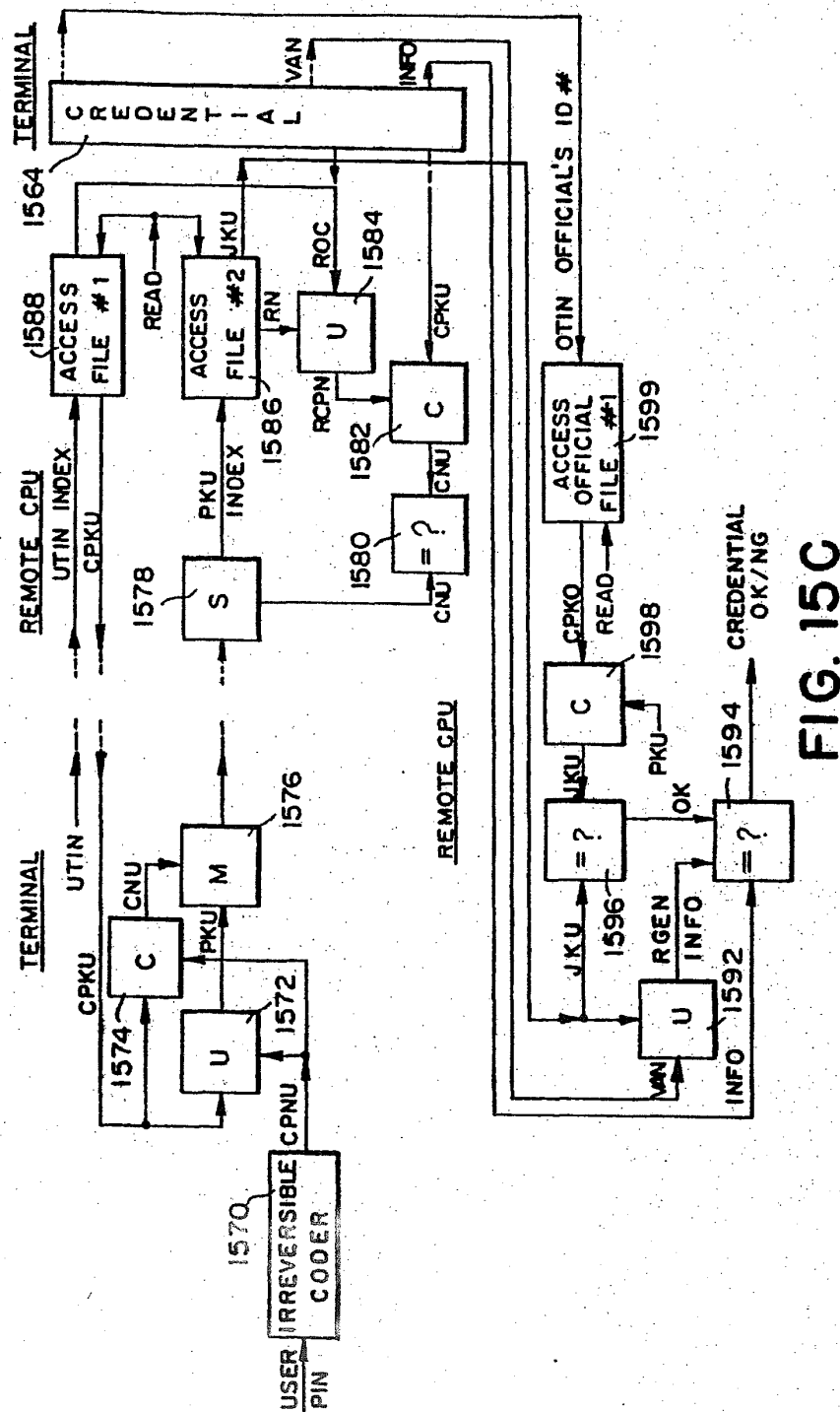
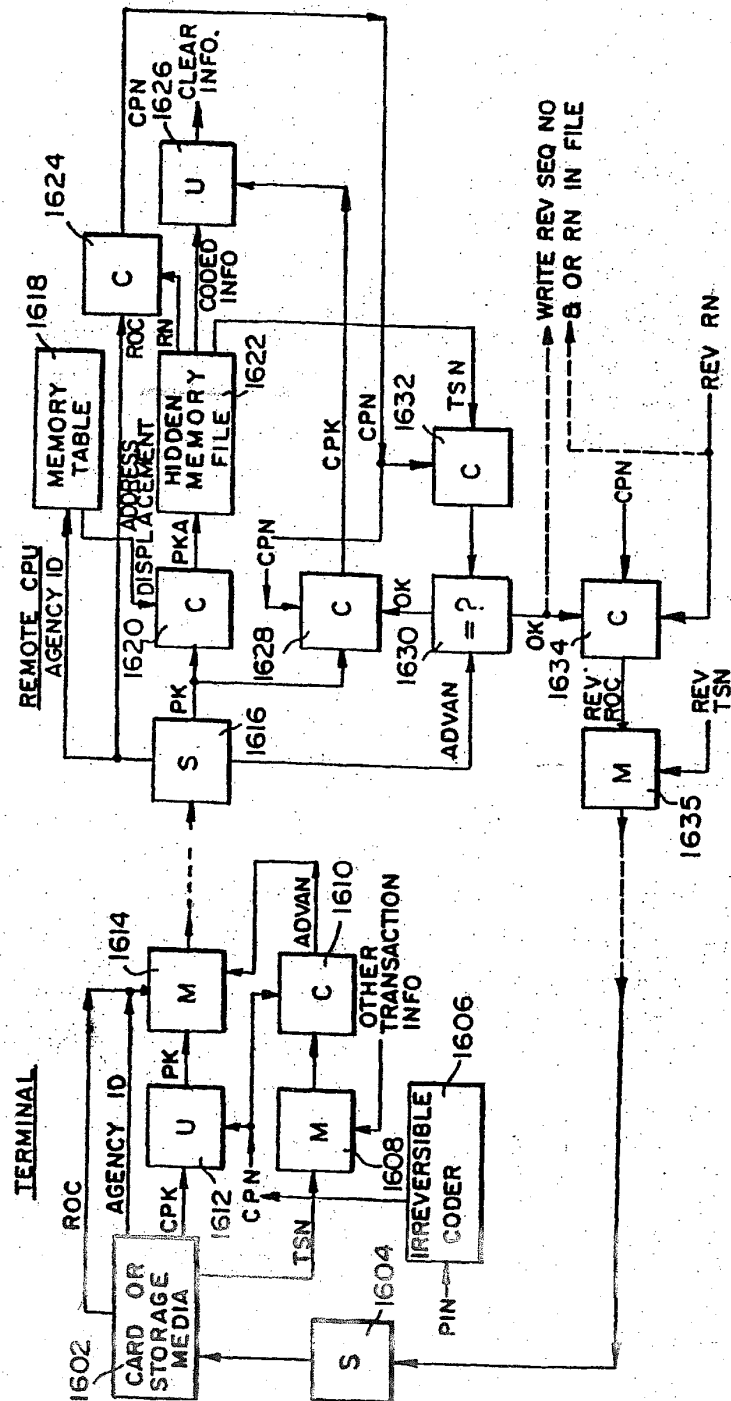


FIG. 15C



SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN

FIELD OF THE INVENTION

The present invention relates generally to secure transaction systems and, more particularly, concerns a method and apparatus for authenticating documents, records and objects as well as the individuals who are involved with them or responsible for them.

BACKGROUND OF THE INVENTION

There are many times in our daily lives when the need arises for highly secure transactions. For example, instruments of commerce, such as checks, stock certificates, and bonds are subject to theft and forgery. From the time a document is issued, the information contained on it, or the name of the recipient could be changed. Similarly, passports, pay checks, motor vehicle registrations, diplomas, food stamps, wager receipts, medical prescriptions, or birth certificates and other official documents are subject to forgery, fraudulent modification or use by an unintended recipient. As a result, special forms, official stamps and seals, and special authentication procedures have been utilized to assure the authenticity of such documents. Medical, legal and personnel records, and all types of information in storage media are also subject to unauthorized access. Passwords and coding of such records have been used to thwart unauthorized access. However, there have always been ingenious individuals who have somehow managed to circumvent or evade all such systems of security.

With the introduction of computers and computer communications into business transactions and document processing, a certain degree of security was gained, in that it is now possible to verify documents and transactions much more quickly, thereby avoiding many frauds which previously went unnoticed until it was too late. However, with the elimination of the human factor, verification of the identity of parties also became more difficult. A pressing need still exists for business transaction, document processing and record access systems which can assure the identity of the parties and the accuracy of the information involved in the transaction. As used herein, the term "record access systems" includes systems which access media which contains data, messages, text, FAX, audio, video, drawings, images, photo, electronic and physical mail, safe boxes, and the like. As used herein the term "business transaction system" will be intended as a generic term to describe all such transaction, document processing and record access systems, including ones not related to business use, such as passport authentication systems.

The security problems described above have been handled with some degree of success in systems involving a single party transaction where the party is present. For example, during the use of an automatic teller machine, the customer is the sole party involved and is present in person. However, until the present invention, it has not been possible to verify the identity and to secure the interests of all parties to multi-party transactions and, in particular, absent parties to a transaction.

SUMMARY OF THE INVENTION

Briefly, the present invention is directed to a transaction, document processing, or record access system which avoids the shortcomings of known systems of

this type. In accordance with an embodiment of the present invention, when a transaction, document or thing needs to be authenticated, information associated with at least one of the parties involved (e.g., an originator and/or a recipient) is coded to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) or code at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. Thus, the joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information. Alternatively, the information could be authenticated by regenerating a VAN from the recorded information and comparing the regenerated VAN with the recorded VAN.

In accordance with an embodiment of the present invention, at the time of enrolling as a user of the system, each user selects a personal identification number (PIN), which is secret, does not exist in an uncoded form, and cannot be recovered from other information anywhere in the system. During or after enrollment, a non-secret identification code and a secret code are also stored in a user's file at the user associated computer facility. When a user participates in a transaction, the user is required to utilize his or her PIN, which after being coded is used to derive a coded arbitrary number. Subsequently, this arbitrary code is compared to another such code which is generated from a reconstituted version of the coded PIN, in order to authenticate the user's identity. One of the embodiments creates a computer file with a secret address to authenticate a user's identity, and to secure sensitive records. The address is preferably not stored anywhere in the system, but is generated when needed from information supplied by the user. In some embodiments of the present invention, when a joint code is created as described above, one participating user (e.g., the originator) must provide his or her PIN. The other party's non-secret identification code and the PIN are utilized in creating the joint code. In other embodiments, the joint code is created from the coded PIN's of the participants.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing brief description as well as further objects, features, and advantages of the present invention will be understood more completely from the following detailed description of the presently preferred, but nonetheless illustrative, embodiments of the invention, with reference being had to the accompanying drawings, in which:

FIGS. 1-5 illustrate the symbols utilized in the present application to represent conventional building blocks used to form the invention, these building blocks being respectively, a coder, an uncoder, a linker, a mixer, and a sorter;

FIGS. 6-8 are functional block diagrams illustrating a check transaction system in accordance with a first embodiment of the present invention, with FIG. 6 illustrating user enrollment, FIG. 7 illustrating how an originator generates a check, and FIGS. 8A and 8B illustrating

ing the authentication process when the check is presented to be cashed;

FIGS. 9-12 are functional block diagrams illustrating a credential issuing and authentication system in accordance with a second embodiment of the present invention, with FIG. 9 illustrating the enrollment of an official, FIG. 10 illustrating the enrollment of a user, FIG. 11 illustrating the issuance of the credential, and FIG. 12 illustrating the authentication of an issued credential;

FIGS. 13A-13E, when arranged as illustrated in FIG. 14, collectively represent a functional block diagram of a check transaction system similar to that of FIGS. 6-8, but including the basic processing necessary to clear and pay a check electronically;

FIGS. 15A-15C are functional block diagrams of a credential issuing and authentication system according to an alternate embodiment of the present invention; and

FIG. 16 is a functional block diagram of a system for authenticating a party and for authorizing access to a secret file associated with the party according to an alternate embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIGS. 1-5 illustrate the functional building blocks utilized in the preferred embodiments. All of these components are conventional building blocks for computer or communication systems. Moreover, those skilled in the art will appreciate that the blocks can be realized as hardware components, or they can be realized as functional blocks in an overall computer program.

The coder illustrated in FIG. 1 and the uncoder illustrated in FIG. 2 may be any form of such device utilizing a known algorithm, such as the Data Encryption Standard (DES). A coder, as illustrated in FIG. 1, has at least one data input, at which it receives clear data. It also has one or more additional inputs for receiving keys K_1 , K_2 , which are utilized to code the clear data into a form in which it could not be easily recognized or decoded without the use of the keys. A variable which is used as a key may be padded to obtain the desired security. An uncoder (FIG. 2) reverses the process of the coder. Basically, it receives the coded data and utilizes the same keys to reconstruct the clear data.

A linker (FIG. 3) receives a plurality of data inputs and concatenates them into a longer code word (D_1 , D_2 , ..., D_N). Similarly, a mixer (FIG. 4) receives a plurality of data inputs (D_1 and D_2 through D_N) and mixes their digits or binary bits. A sample example of a mixer would be a conventional time division multiplexer which is used to interleave plural data inputs. However, in many applications, it will be preferable to utilize a more sophisticated mixer, such as one that utilizes arithmetic and logical combinations of digits or bits. A sorter (FIG. 5) reverses the process of a linker or a mixer, that is, it receives a concatenated or mixed code word and reproduces the original component words. A time division de-multiplexer could serve as a sorter for a mixed signal originally generated by a multiplexer.

FIGS. 6, 7, 8A and 8B constitute a functional block diagram illustrating the present invention in a check transaction system. The system illustrated in FIGS. 6, 7, 8A and 8B are well suited for use in generating and processing employee paychecks, for example. The system involves three phases of operation. In the first phase, illustrated in FIG. 6, a user of the system must enroll in order to be recognized by the system. Each

user enrolls at his or her bank, or at another convenient location, such as a place of employment, in the presence of an officer, who appropriately verifies the user's identity and obtains the typical information from him, including his taxpayer identification number (TIN) and telephone number. An account is then opened for the user and a file is created for him or her in the bank's computer, and the bank assigns a person account number (PAN) to the user's account. If a bank card is issued to the user, it usually contains the PAN and a bank identification number (BIN).

While operating a terminal, the user is requested to select a personal identification number (PIN) and to enter that PIN into the terminal. The user complies and such entry occurs at block 10 of FIG. 6 with the typical transaction information, including the user's TIN or PAN, being entered at block 11. The PIN is applied directly to an irreversible coder 12, where it is processed to produce a coded PIN (CPN). Coder 12 may be any type of conventional coding device which can process the PIN so that the coding is irreversible (i.e., the PIN cannot be recovered from the CPN). At the same time, a random number generator 14 produces a random number (RN), which is applied to a mixer 16 along with the CPN. Alternately, the user may be permitted to select an arbitrary number for RN.

The signal produced by mixer 16 is then transmitted to the bank's computer, where it is applied to a sorter 18. It is assumed that this transmission preferably occurs over a secure line, such as one protected by a tandem coder and uncoder which can utilize a joint terminal-bank key. The sorter recovers the original CPN and RN, saving RN in the user's file at block 22. It should be noted that in saving RN, the user's file is accessed by using his TIN as an index. The received CPN is applied as the data input to a coder 20, which receives RN as its key input, producing a revisable owner code (ROC) which is saved in the user's file in the same manner as RN. Various additional information is saved in the user's file, such as his personal account number (PAN), name, phone number (PHN), account balance, and other relevant information. The user's TIN, PAN or PHN can be used as an index to access the user's file. CPN represents coded authentication information since it is a coded form of the PIN, and since it is used in other parts of the system to authenticate the user and the transaction. The system preferably maintains RN as a secret number (although in the present embodiment the user file is not secret since it is accessed using a non-secret index) and ROC is maintained as a non-secret number. As explained in detail below, CPN is derivable from ROC and RN.

FIG. 7 illustrates how the originator generates a check in accordance with the present invention. This process preferably takes place at the originator's terminal or computer. It is assumed that the originator would be generating a check in the usual manner and would include on it all of the information usually found on a check, as well as the information normally recorded or imprinted on check forms, such as the recipient's name and TIN (RTIN), and the originator's personal account number and bank identification number. Preferably, the terminal includes a check reader and printer which can read necessary information from the originator's check form and print information on the form, although this could also be done manually by the originator. The originator and the recipient can be the same person, for example, where a person is cashing a personal check

originated by the person. In the case of multi-party checks, the check is originated by a present party (i.e., the originator) in favor of an absent party (recipient).

The originator enters his or her PIN at a terminal or computer. Through irreversible coder 10, the originator's PIN is converted to a coded PIN (CPNO), which is applied as the key input to coder 28. The data input to coder 28 is the recipient's TIN (RTIN), which has been read from the check, or accessed from the computer memory, or entered by the originator. The data output of coder 28 is a joint key (JK), which is applied as the key input to a coder 30. Generally, the JK is generated using information associated with at least one of the parties involved in the transaction (in this case, the originator and recipient). As will be shown more fully below, the joint key (or code) is used to protect and authenticate the originator and recipient. The data input to the coder 30 is the information (INFO) to be authenticated (that is, information relevant to the transaction, such as check number, amount, etc.).

The data output of the coder 30 is a variable authentication number (VAN), which codes the information to be authenticated, based upon information related to the recipient and information related to the originator. Note that the VAN is alternatively generated directly from INFO and information associated with at least one of the parties, without the intermediate step of generating the JK. The VAN and at least a portion of the information relevant to the transaction are written or imprinted upon the check 32, thereby becoming a permanent part of it. Alternately, the check may represent an electronic transfer of funds or some other type of electronic transaction. In this case, the VAN and at least a portion of the information relevant to the transaction are included with the electrical signals associated with the electronic transaction.

It is contemplated that in creating the VAN, all information would not necessarily be coded in the same manner. For example, the amount of the check might be considered important enough so as to be recoverable completely, and it would be coded into the VAN in a manner that would permit complete recovery. Other information, such as the date and check control number might be considered less important and would be coded into the VAN in such a manner as to permit detection of changes (e.g., error detection coding), but without complete recovery of the original information.

As noted above, other predetermined information which is known jointly by the originator and recipient, and which does not appear on the check, can also be used to derive the VAN. For example, when a check is drawn to multiple recipients, e.g., husband and wife, each recipient's TIN (which does not appear on the check) may be used to derive the joint code and VAN. This makes it more difficult to fraudulently generate the VAN since the predetermined information not appearing on the check would not be generally known.

FIGS. 8A and 8B illustrate the authentication process at a terminal when the recipient presents the originator's check to be cashed. The terminal communicates via a network of the banks involved in the transaction. Preferably, the terminal includes a device which can read information directly from the check 32. Alternately, the terminal operator can manually key information into the terminal, based upon information appearing on the face of the check 32. At block 40, the recipient inserts his or her PIN, and at block 41, identifies his bank and enters his TIN (RTIN) and all information

required by the terminal to initiate the transaction. An irreversible coder 42 processes the PIN to produce the coded PIN, CPNR, which is applied as the key input to a coder 44. A random number generator produces a random number (i.e., an arbitrary number) RNX which is applied as the data input to coder 44. Coder 44 then produces a coded random number (i.e., a coded arbitrary number), CRNX, which is applied to mixer 48 along with RNX. The output of the mixer is, therefore, a signal which contains CRNX and RNX in a converted form, so that neither number nor CPNR may readily be discerned from the signal. CRNX represents coded authentication information because it is a coded representation of CPNR, and because it is used by the system to authenticate the recipient and the transaction.

The mixer signal, along with the information entered in block 41 and the information read from the check are transmitted to the computer at the recipient's bank (i.e., remote bank CPU) over preferably an unsecured line (the use of an unsecured line is possible because CRNX and RNX, not CPNR, are transmitted from the mixer 48 to the sorter 62). The system first authenticates the identity of the check holder at the recipient's bank. Next, the information on the check, as well as the originator and recipient, are authenticated at the originator's bank.

At the recipient's bank, the output of mixer 48 is received in a sorter 62, which separates CRNX and RNX, with CRNX being applied to a comparison block 64 and RNX being applied as the data input to a coder 66. Based upon the recipient's TIN, RTIN, his bank's computer is able to access his file at block 68 and to extract his ROC (a non-secret number) and RN (a secret number), ROCR and RNR therefrom. ROCR and RNR are applied as the data and key inputs, respectively, to an uncoder 70, which generates the recipient's CPN, CPNR, which is applied as the key input to coder 66. Coder 66, therefore, reproduces the recipient's coded random number, CRNX (in the same manner as coder 44), which is applied as the second input to comparison block 64. It should be appreciated that the CPNR output of uncoder 70 is the true CPNR derived from the bank's records. Accordingly, the CRNX produced by coder 66 is the true CRNX. Therefore, should the comparison at block 64 fail, the authentication of the recipient has failed and it is presumed that recipient is not the party presenting the check. The transaction is therefore aborted. On the other hand, if the recipient's identity is authenticated, the transaction can proceed. The recipient's bank then communicates with the originator's bank, conveying all the information about the transaction and requesting authorization to pay (block 74).

As shown in FIG. 8B, at the originator's bank, using OTIN (or the originator's PAN) as an index, the originator's ROCO and random number, RNO, are extracted from the originator's file at block 50. ROCO is applied as the data input to an uncoder 52, and RNO is applied as the key input to uncoder 52. Uncoder 52 therefore reverses the operation performed by coder 20 (FIG. 6) when the originator enrolled, producing the originator's CPN, CPNO. CPNO is then applied as the key input to a coder 56, which receives the recipient's TIN, RTIN, as the data input.

In accordance with the embodiment just described, it is contemplated that security considerations may warrant revising the ROC from time to time independent of any transaction. Toward this end, CPN could be reconstructed from the current ROC and RN as in block 52.

Next, a new RN is used with CPN to generate a revised ROC, making use of a coder in the same manner as coder 20 of FIG. 6. The user's new RN and ROC are stored and accessed, and CPN need only be reproduced at the bank where the user maintains an account.

In the same manner as coder 28 of FIG. 7, coder 56 therefore produces the joint key JK. JK is applied as the key input to an uncoder 58, which receives the VAN from check 32 as its data input. Uncoder 58 therefore reverses the coding operation performed by coder 30 of FIG. 7. If the information on the check has been unmodified, the coder 58 should therefore reproduce the information INFO from the check which was sought to be authenticated. In block 60, a comparison is made between the output of uncoder 58 and the information appearing on the check. Failure of this comparison is an indication that the check may have been modified after being issued, and the originator's bank notifies the recipient's bank that the check will not be honored. Alternatively, the joint key JK from the coder 56 can be used to code the information (INFO) from the check to generate a new VAN, which can then be compared with the VAN from the check to authenticate the check.

Should the comparison be favorable, this is an indication that the check is authentic and unmodified, and the originator's bank accesses the originator's account (block 61) to determine if the account is in order and has sufficient funds or credit to pay the check. The date of the check is determined to be acceptable. If the check control number does not appear in the originator's file as a previously cashed check, then the current check control number is saved to prevent fraudulent check reuse. The originator's bank generates a redeemed or redemption VAN (RVAN) in coder 54, using its bank key and the original VAN. RVAN is saved in the originator's file (block 55) and is recorded on the check (block 57). The originator's account is then debited. The originator's bank then authorizes the recipient's bank to pay the check. On the other hand, if originator's bank finds any irregularity in the check or in the originator's account, it will notify the recipient's bank that the check is dishonored.

The RVAN (and other RVAN's from other transactions) can be accessed from originators, files by banks and other financial institutions involved with processing checks to determine the status of checks. Thus, by creating and storing the RVANs in the originators' files, fraudulent reuse of checks is avoided.

At block 72 (FIG. 8A), the recipient's bank receives the originator's bank's instructions. It will then notify the recipient if the check has been dishonored. If the check has been honored, the recipient's account may be credited as in a deposit. Alternately, the recipient can receive payment immediately if he is at an appropriate terminal, such as an automatic teller machine.

Essentially, the check has cleared automatically, online, without further check handling or processing.

In a transaction where the user cashes his own personal check, the originator and recipient are one and the same. A VAN is created from a joint code which combines information associated with the user, such as the user's identification number (TIN or PAN) and the user's CPN, which is generated directly from a PIN entered by the user. When the VAN is authenticated, the joint code is derived by combining the user's identification number (TIN or PAN), and the user's true CPN, which is generated from the RN and ROC re-

trieved from the user's file, with the TIN (or PAN) serving as a file index.

As noted above, in FIG. 8A it is possible to use an unsecured link between the mixer 48 and the sorter 62 because CRNX and RNX, not CPNR, are transmitted from the mixer 48 to the sorter 62. However, a security problem still exists in using an unsecured line between the mixer 48 and the sorter 62 because the signal can be recorded and then played back later to attempt to fraudulently authenticate a fraudulent transaction. In an alternate embodiment of the present invention, an anti-duplication variable authentication number (ADVAN) is generated at the recipient's terminal by coding at least a transmission date and time with the CPNR by a coder (not shown). The ADVAN is then mixed with the CRNX and the RNX by the mixer 48 and sent to the remote bank CPU over the unsecured line to the sorter 62. At the remote bank CPU, the CPNR which is generated by the uncoder 70 is used to uncode the ADVAN to regenerate the transmission date and time. The signal received over the unsecured line is then authenticated by comparing the regenerated transmission date and time to a reception date and time (that is, the date and time at which the signal was received at the remote bank CPU). In this manner, the recipient and transaction are further authenticated.

According to another embodiment of the present invention, RNX is generated at both the recipient terminal and the remote bank CPU. To generate the RNX at the remote bank CPU, a random number generator is located at the remote bank CPU, wherein the random number generator at the remote bank CPU is similar to and synchronized with the random number generator 46 located at the recipient's terminal. Instead of transferring the RNX and the CRNX, only the CRNX is transferred over the unsecured line from the recipient's terminal to the remote bank CPU. At the remote bank CPU, the CPNR generated by the uncoder 70 is coded by the coder 66 with the RNX generated at the remote bank CPU to generate the CRNX. The generated CRNX is then compared by the comparator 64 with the CRNX transferred from the recipient's terminal to the remote bank CPU to authenticate the recipient and the signal received over the unsecured line. In this manner, the recipient and transaction are further authenticated.

According to another embodiment of the present invention, CRNX is never generated. Instead, the CPNR generated by the irreversible coder 42 is sent to the remote bank CPU over a secured line, rather than over an unsecured line. The CPNR generated by the uncoder 70 is then compared by a comparator (not shown) with the CPNR sent from the recipient's terminal to the remote bank CPU to authenticate the recipient. In this alternate embodiment, the random number generator 46, coder 44, mixer 48, sorter 62, and coder 66 are not required, although a secure line is required.

FIGS. 9-12 constitute a functional block diagram illustrating the present invention in a credential issuing and authentication system. The system involves the same three phases of operation as the check transaction system of FIGS. 6, 7, 8A and 8B. However, all users are enrolled by an authorized official who must be enrolled first. Accordingly, there are two enrollment processes which are somewhat different. The first one is enrollment of the official, and the second one is enrollment of a user prior to or at the time of issuing his credentials. It is contemplated that this system would be useful for all types of credentials and records; for example, motor

vehicle registrations, social security cards, passports, birth certificates and all types of identification cards or personal storage media. This system would also be useful in protecting against unauthorized access to all types of records, as previously indicated.

FIG. 9 illustrates enrollment of the official. This can be accomplished at a terminal or computer which is in communication with a remote computer over a link which is assumed to be secure. The remote computer may, for example, be the central computer at the agency issuing the credential. At the remote computer, number generator 100 generates a random number which, at block 102, is compared to a current list of all assigned personal keys. If the random number does not correspond to an assigned personal key, then the random number is assigned as the personal key, PKO, of the official being enrolled. Alternatively, PKO can be selected at random, from a list of unused PKO's, and the list of available PKO's would thereby be diminished. In yet another alternative, PKO could be accessed from a counter, such as a pseudorandom or an ordinary sequential counter the output of which may be coded with a secret key. The size, or length, of PKO can be such as to provide a full size memory address or an offset or an index extension, to limit or enlarge the memory space wherein concealed files are stored. PKO is then transmitted over the secure link to the enrollment terminal.

At the terminal, the official enters his PIN and name and various other information required by the system. The name can be numerically coded by using a telephone type key pad. The PIN is applied to an irreversible coder 104, which produces his coded PIN CPNO. CPNO is applied as the key input to a coder 106, which receives PKO as the data input. The data output of coder 106 is the official's coded personal key, CPKO, which is applied as an input to mixer 107. The official's name code and TIN, OTIN, are also applied as inputs to mixer 107. CPKO represents a coded address since it is a coded representation of PKO.

The output of mixer 107 is transmitted back to the remote computer over the secure link. At the remote computer, sorter 109 separates the received signal into its component parts: CPKO, the official's name code, and OTIN. At block 108, CPKO and the official's name code are then saved (i.e., written) into File No. 1 assigned to the official with the official's TIN, OTIN, serving as a File No. 1 index. It is assumed that during the official's enrollment various other information will be provided by the official over the secure line and may be stored in his File No. 1. It should be noted that OTIN is not secret and, therefore, the location of File No. 1 and the contents of File No. 1 (including CPKO) are not secret.

At block 112, PKO is used as an index for File No. 2, which is also allocated to the enrolling official. The location of File No. 2 (and thus, the contents of File No. 2) is concealed, since PKO is secret and not stored anywhere in the system. The information or records which are stored in File No. 2 can be coded or uncoded. The memory space wherein concealed files are stored may be previously filled (or pre-loaded) with dummy or false information to make the contents and locations of authentic allocated files undistinguishable from the dummy files. The concealed File No. 2 can also be used to store the ROC and RN (or store only RN, since only RN is secret—ROC could be stored in a non-secret file, such as Official's File No. 1), as previously described in

FIGS. 6, 7, 8A and 8B, to reconstitute a user's coded PIN, CPN. The concealed File No. 2 can also be used to store other secret information (not shown) associated with the official. An official's coded number, CNO, is generated at the output of coder 110, and is saved in File No. 2 at block 112. The key input to coder 110 is CPKO and the data input to coder 110 is PKO or an arbitrary predetermined number (APN). CNO represents coded authentication information because it is a coded representation of CPKO, and because it is used by the system to authenticate the official.

At coder 110, CPKO and PKO can be interchanged as the key and data inputs. However, the arrangement selected must then be used consistently in each phase of the operation of the system.

Those skilled in the art will appreciate that the present embodiment offers an additional level of security in that, not only is secret information unavailable to a person who does not know the related PK and PIN, but that person is even unable to determine the location of the file containing the information, and is unable to uncode the information contained therein.

FIG. 10 illustrates user enrollment. The user is enrolled by a previously enrolled official, who verifies the user's identity, based on acceptable documentation. Before the user can be enrolled, the official's identity and authority are preferably authenticated. The official operates the terminal, where he enters his PIN, and his TIN, OTIN, and the name code used during his enrollment, which was stored in his "File 1". OTIN is transmitted to the remote computer, where it is used as an index to access CPKO from the official's File No. 1, and CPKO is returned to the terminal. The official's PIN is applied to the irreversible coder 104, which produces CPNO. CPNO is applied as the key input to an uncoder 114, which receives CPKO as a data input over the secure link from the remote computer. It will be appreciated that uncoder 114 simply reverses the process of coder 106 of FIG. 9, therefore producing PKO. PKO is applied to a mixer 118, the other input to which is the official's name code. The output of mixer 118 is then transmitted to the remote computer.

At the remote computer, the signal transmitted from mixer 118 is received in a sorter 124, which separates out PKO, and the name code. The extracted PKO is utilized as an index to address the official's "File 2" whereby CNO is read. The CNO read from File No. 2 is compared against the CNO generated by coder 120, which has as its data input PKO which is extracted by sorter 124 and as its key input is CPKO read from "File 1". Should this comparison fail, the identity of the official is not authenticated and the enrollment of the user is aborted. Assuming that the comparison is successful, comparator 130 is then enabled. At block 130, the name code which is extracted from sorter 124 is compared against the name code read from the official's "File 1" (using OTIN as index). Should this comparison fail, the enrollment of the user is aborted. Should the comparison be successful, the official has been fully authenticated and the user's enrollment may proceed.

At the remote computer, number generator 100 generates a unique random number, which is assigned to the user as a personal address key, PKU. Alternately, PKU can be generated from a counter as previously described. As discussed below, PKU represents a predetermined secret address of a File No. 2 associated with the user. PKU is transmitted over the secure link to the

enrollment terminal, where it is applied to the data input of coder 113.

The user operates the terminal and selects a PIN which he enters along with his TIN, UTIN. The user's PIN is applied to the irreversible coder 104, which produces the user's coded PIN, CPNU. CPNU is applied as a key input to coders 113 and 115. The output of coder 113 is the user's coded personal key, CPKU (which represents a coded address of the user's File No. 2), which is applied as a data input to coder 115. The output of coder 115 is the user's coded number, CNU, which is applied to the input of mixer 116. The user's TIN, UTIN and CPKU are also applied as inputs to mixer 116. The output of mixer 116 is transmitted back to the remote computer over the secure link. CNU represents coded authentication information because it is a coded representation of CPKU, and because it is used by the system to authenticate the user.

At the remote computer, sorter 119 separates the received signal into its component parts: CPKU, CNU and UTIN. At block 108, CPKU and CNU are saved (i.e., written) into File No. 1 assigned to the user, with the user's TIN, UTIN serving as a File No. 1 index. It should be noted that CPKU and CNU may be recorded on the user's credential when they are generated at the terminal. It should also be noted that UTIN is not secret, and therefore, the location and contents of the user's File No. 1 are not secret. It should further be noted that the official's CNO is stored in the official's secret File No. 2 (FIG. 9) while the user's CNU is stored in the user's non-secret File No. 1 (FIG. 10A), even though both CNO and CNU are used to authenticate the official and the user, respectively. These two different ways for storing CNO and CNU (as shown in FIGS. 9 and 10A) illustrate two embodiments of the present invention.

The user's PK, PKU (or an arbitrary predetermined number APN), is applied as the data input to a coder 132, which receives the official's CPKU as a key input. Coder 132 produces a joint key, JKU, which it will be appreciated, is determined by information related to the user and information related to the official. Using PKU as an address, the joint key is written into the user's "File 2" at block 112, and using PKO and UTIN as address indices, the joint key JKU is written into the official's "File 2" at block 134 (FIG. 10B). These writes are enabled as a result of the success of the comparison occurring at block 130. Accordingly, the user's "File 2" will contain a joint key, and the official's "File 2" will contain a joint key for each user the official enrolls. Since the user's file 2 is addressed by PKU (which is secret), the location and contents of the user's file 2 are secret. At coder 132, when the joint key JKU is generated, CPK and PK can be interchanged as key and data inputs, or as to user and official inputs. However, the arrangement selected must then be used consistently.

FIG. 11 illustrates issuance of the credential. This is shown separate from the user enrollment process of FIG. 10. However, in many instances, it would occur at the same time. In the preferred embodiment, this process is shown as occurring at the agency's computer, although it may be performed by the official from a terminal where he may communicate with the computer. It is assumed that the official has a credential printer or recorder which contains credential forms on which information is printed or recorded to produce the actual credential. However, it is also possible to create the credential by inserting information manually or on a

typewriter, provided the necessary information derived by the system can be entered. The official enters the usual information (INFO) normally contained on a particular credential 145. The user's TIN may also be recorded on the credential. Alternately, the user's CPKU and CNU may be recorded on the credential, after being extracted from the user's File No. 1, with UTIN serving as a file index. If CPKU and CNU are recorded on the credential, they may be erased from the user's File No. 1. Alternatively, only CNU may be recorded on the credential, with CPKU remaining in File No. 1, or vice versa.

The issuing process continues with the official entering his PIN, which is applied to an irreversible coder 140 to produce his CPNO, which is applied as a key input to an uncoder 142. At block 144, the official's TIN, OTIN is utilized as an index to access the official's "File 1", so that CPKO may be read therefrom and applied as the input to uncoder 142. Uncoder 142 therefore performs the same process as uncoder 114 of FIG. 10 to produce PKO. At block 146, PKO and UTIN are utilized as address indices to access the official's "File 2" and JKU is read therefrom. The information INFO on the credential is applied as the data input to a coder 152 and JKU is applied as the key input, whereby coder 152 codes the INFO to produce a VAN, which is recorded on the credential. After recording the VAN on the credential, the joint key, JKU, may be erased from the official's File 2, where it was stored (or held in escrow or in trust), until the credential was issued. Alternately, the authentic JKU may be replaced with a false or dummy JK for security purposes. This completes the issuance of the credential 145. It should be noted that the joint key JKU stored in the official's File No. 2 can only be used in a transaction if a party exists with knowledge of the official's PIN, since this PIN is required to access the official's File No. 2 (at block 146). Thus, a person who does not have knowledge of the official's PIN (such as an unscrupulous person trying to issue a fraudulent credential) cannot legitimately issue a credential.

The VAN which is generated from information (INFO) recorded on the credential, or from information which is otherwise stored by the system, can include (coded) personal descriptive details to further identify the user (in addition to the user's PIN and TIN) in order to limit the use of the credential to the sole individual to whom it was issued (or sold). Thus, items such as bank cards, tickets, green cards, food stamps, ballots, travel checks, FAX messages, etc., can be protected and used solely by the individuals to whom they were issued. Also, the use of the credential may be enlarged to include a group, such as a family, by coding such information into the VAN.

FIG. 12 illustrates the authentication of an issued credential. This is preferably performed at a terminal provided for that purpose. The terminal includes a reading device for the credential 145 and an input device, such as a keypad for the user. The information could, however, be read from the credential and keyed in by hand. The terminal communicates with the remote processor via a preferably secure link.

As part of the credential authentication process, the identity of the user is authenticated. This requires that the user enter certain information at the terminal, including a PIN and user's TIN, UTIN, which is transmitted to the remote computer, which returns CPKU and CNU (box 178) via a secure data link. Alternatively,

13

CPKU and CNU could have been recorded on the credential (or on some other item in the possession of the user, such as a card having a magnetic stripe for storing data) and inputted directly into the terminal. The PIN is applied to the irreversible coder 170 which produces CPNU. CPNU is applied as the key input to coder 172 and uncoder 174. Coder 172 receives CPKU as a data input. It should be noted that coder 172 performs in the same manner as coder 115, which produced CNU at its output during the user's enrollment. The output of coder 172 is applied as an input to the comparator at block 182, which also has as an input the CNU extracted from the user's File No. 1 (or inputted from the user's credential).

Should this comparison fail, the identity of the user is not authenticated, and the credential authentication is aborted. Assuming the comparison is successful, the user is identified, and the credential authentication, with access to the hidden File No. 2, ensues. The favorable output from comparator 182 enables uncoder 174. The data input to uncoder 174 is the user's CPKU. The key input to uncoder 174 is the user's CPNU, as already explained. It will be appreciated that uncoder 174 simply reverses the process of coder 113 of FIG. 10, therefore producing PKU. PKU is applied to a mixer 176 which also receives the VAN and INFO of the credential. The output of mixer 176 is then transmitted to the remote computer over the secure link.

At the remote computer, UTIN is utilized as an index to access the user's "File 1" at block 178. This permits reading of CPKU and CNU from the file, whereby CPKU and CNU were transmitted back to the user's terminal. At the remote computer, the signal transmitted from mixer 176 is received in sorter 180, which separates out PKU, VAN and INFO. The extracted PKU is utilized to address the user's "File No. 2" at block 184 whereby JKU is read. It will be appreciated that the user's File No. 2 has been accessed by an authorized user without reference to, or use of, information stored in the file. The VAN extracted from sorter 180 is applied as a data input to an uncoder 162, which receives the joint key JKU extracted from the user's "File 2" at block 184. It will be appreciated that uncoder 162 therefore reverses the process performed by coder 152 of FIG. 11. Assuming the VAN on the credential is the same one as originally recorded, uncoder 162 will have produced the recovered INFO which should be the same as the actual INFO recorded on the credential.

At block 169, the INFO from the credential is compared to the INFO recovered from uncoder 162. Should the comparison fail, this is an indication that INFO on the credential has been modified, and the credential is indicated as not being authentic. Should the comparison be successful, this is an indication that INFO is accurate, and the authenticity of the credential is confirmed. Alternatively, the credential information from the credential is coded using the JKU from the user's File No. 2 to generate a new VAN, which is compared with the VAN from the credential to authenticate the credential.

In order to enhance the security of this system, it would be desirable to make unassigned areas of memory indistinguishable from those utilized to store information for the "File 1" and "File 2" information. This is accomplished by pre-storing pseudo-information in unused memory allocated as hidden memory space. This pseudo-information constitutes random information arranged in the same format as actual files. This

14

prevents an intruder from searching memory for structures that look like actual information files and using the uncovered information to work backwards to breach security.

FIGS. 13A-13E, when arranged as shown in FIG. 14, constitute a functional block diagram illustrating further aspects of the check transaction system of FIGS. 6, 7, 8A and 8B. Specifically, these figures illustrate a three-party check transaction, with each of the participants and the fidelity of the information on the check being authenticated, the check being automatically cleared, and the funds of the participants being immediately credited or debited, all of these processes being performed on-line. The participating parties in this transaction are the check originator, whose account is to be debited; the check recipient to whom the check is drawn; and the check redeemer, who is cashing the check for the recipient or accepting it in payment for goods or services, and whose account is to be credited. In addition, the banks for each of these participants will also be participating in the transaction, and the messages generated by these banks will be authenticated. It is assumed that any individual or bank participating in the system will have enrolled as illustrated in FIG. 6. In addition, it is assumed that a check used in the system is generated in the manner illustrated in FIG. 7.

Referring first to FIG. 13A, the recipient of the originator's check has presented the check to the redeemer (block 200). The recipient and the redeemer are at a terminal which includes appropriate input means 202. Preferably, the input means includes a check reader and a keypad for each of them. However, in the absence of a check reader, it is also possible to key in information from the face of the check. The check is examined to determine if it contains a redemption VAN from a previous transaction. The presence of a redemption VAN is an indication that the check was used previously, and it will not be honored. If a redemption VAN is not present, then the transaction can proceed. It is assumed that the redeemer's bank identification number (RDBIN), and TIN are stored in the terminal, otherwise the redeemer keys in his bank's name and TIN, and the recipient keys in his TIN, PIN and bank's name. A bank directory is addressed at block 203 to produce the recipient bank's identification number (RCPBIN). The recipient's PIN is applied to an irreversible coder 42, which produces his CPNR. Irreversible coder 42, coder 44, random number generator 46, and mixer 48 are the same components illustrated in FIG. 8A and cooperate in the same manner to produce RNX, CRNX, in a mixed form at the output of mixer 48.

The terminal has available to it the redeemer's bank key (RDBK), which is applied to the key input of a coder 204, the data input to which is the terminal ID (TID), which is generated by the terminal. Coder 204 then produces a joint terminal bank key (JTBK), which is applied as the key input to a coder 206, the data input to which is the output of mixer 48. The mixer output is therefore coded with a joint key JTBK which has been generated on the basis of information related to the redeemer's bank identity and the terminal identity.

The output of coder 206 and the information from input means 202, and the recipient's TIN, RCPBIN, and the recipient's bank ID number, RCPBIN, are then transmitted to the computer at the redeemer's bank. At the redeemer's bank (FIG. 13B), all of the received information is placed in temporary storage (block 208).

15

The redeemer's TIN, RDTIN, (originally stored in the terminal, or keyed in by the redeemer), is then utilized as an index to access his account file, at block 210.

The check control number (CCN) of the present check is then compared to the CCN's stored in the redeemer's file during previous transactions (block 212), and the transaction is terminated if the present CCN matches that of a previously processed check. If the CCN of the present check is not a duplicate, processing continues.

RDBIN, and RCPBIN are utilized as indices to access a bank key table (block 213), which produces the redeemer's bank key RDBK, and the recipient's bank key RCBK, which are applied as the data and key inputs, respectively, to a coder 214. The coder 214 then produces a joint bank key JBK, which is derived from information related to the identity of the redeemer's bank and the identity of the recipient's bank.

The terminal identification (TID) is input to a coder 216, which has as a key input RDBK. In the same manner as coder 204, coder 216 therefore produces JTBK, which is applied as a key input to an uncoder 218. The data input to uncoder 218 is the information in temporary storage 208 which was originally received from coder 206. Coder 218 therefore reverses the process performed by coder 206, yielding the output of mixer 48, which is applied as a data input to a coder 220. The key input to coder 220 is JBK, so that the output of mixer 48 is now coded with the joint bank key JBK. The output of coder 220 is then transmitted in a message to the recipient's bank, along with RCPTIN, RDBIN, and RCPBIN.

At the recipient's bank, the received information is saved in temporary storage 230. RCPBIN and RDBIN are then applied to a bank key table (block 232), to yield RCBK and RDBK, which are applied as the key and data inputs, respectively, to a coder 234. In the same manner as coder 214, coder 234 therefore yields the joint bank key JBK, which is applied as a key input to uncoder 236. The data input to this uncoder 236 is the coded combination of RNK and CRNK produced by coder 220. Uncoder 236 therefore reverses the process of coder 220, yielding the mixture of RNK and CRNK as an output. This mixture is applied as an input to a sorter 238, to recover RNK and CRNK.

The recipient's TIN, RCPTIN, is utilized as an index to access the recipient's file at block 240 and read therefrom the random number, RNR, and his ROC, which are applied as the key and data inputs, respectively, to an uncoder 242. In the same manner as uncoder 70 of FIG. 8A, uncoder 242 therefore derives the true CPNR, which is applied as a key input to a coder 244, which receives RNK as a data input. The data output of coder 244 is therefore the true CRNK.

At block 246, this true CRNK is compared to the CRNK derived from sorter 238. If this comparison is favorable, the recipient's identity is confirmed, and processing may proceed. Otherwise, processing is terminated, with the originator's check being dishonored, because the recipient has not been properly authenticated. The recipient's bank then transmits a message to the redeemer's bank, informing it whether or not the recipient has been authenticated. If the recipient has not been authenticated, the redeemer's terminal is notified, and processing will terminate.

Assuming that the recipient has been authenticated, the recipient's bank message includes various information which is temporarily stored by the redeemer's bank

16

(block 250 of FIG. 13C). At block 252, the originator's bank identification number ORBIN, which was read from the check, and the redeemer's bank identification number RDBIN are applied as indices to a bank key table to recover bank keys for these banks, OBK and RDBK, respectively. These keys are applied to a coder 254 to produce a joint bank key JBK', which is therefore dependent upon information related to the originator's bank and the information related to the redeemer's bank. JBK' is applied to the key input of a coder 256, which receives the original VAN, OVAN, (from the check) as a data input. The output of coder 256 is a redeemer's bank RDBVAN, which is transmitted to the originator's bank, along with various transaction information and the information from the check. RDBVAN serves to authenticate the communication between the banks.

At the originator's bank, the received information is temporarily stored at block 258. ORBIN and RDBIN are then utilized to reference a bank key table at block 260, whereby OBK and RDBK are extracted in the same manner as in block 252. The joint key JBK' is then generated by means of a coder 262 in the same manner as coder 254. JBK' is then applied as the key input to an uncoder 264, which receives RDBVAN as a data input. This uncoder 264 therefore reverses the process performed by coder 256 and produces an extracted OVAN, which is applied to a comparator 266 (as shown in FIG. 13D).

The originator's personal account number ORGPAN which originally appeared on the check is utilized as an index to access the originator's account file at block 268 of FIG. 13C. This provides access to various information about the originator's account including the balance and a list of prior check control numbers (CCN's), and in addition, provides access to his revisable owner code ROCO and random number RNO, which are applied as the data and key inputs to an uncoder, to produce the originator's coded pin CPNO. CPNO is then applied as the key input to a coder 272 (FIG. 13D) which receives the recipient's TIN, RCPTIN, as a data input. The output of coder 272 is the joint key JK, which is applied as the key input to a coder 274, which receives the check information as a data input. It will be appreciated that coders 272 and 274 regenerate the original VAN, OVAN, from the check in the same manner as coders 28 and 30 of FIG. 7. This regenerated VAN is then compared to the extracted VAN at block 246. If this comparison fails, it is an indication that the check information may have been tampered with and the originator's bank informs the redeemer's bank that the check will be dishonored. On the other hand, if the comparison succeeds, the process continues.

The originator's bank then performs a series of computations, including determining whether the CCN of the check is proper (i.e., has not been used before) and whether the originator has a sufficient balance in his account (or credit) to cover the check, and whether the date of the check is acceptable. In the case of any defects, the check will be dishonored and the process will terminate. Assuming that everything is in order, modification of the originator's account is approved, and a record of the check created at block 271, with the new information being added to temporary storage at block 273. Coders 275 and 276 are then utilized to encode the original VAN, OVAN, into an originator's bank VAN OBVAN. Various information about the transaction,

and authorization to credit the redeemer's account are then transmitted is a message to the redeemer's bank.

At the redeemer's bank, all of the received information is stored in temporary storage at block 278. At block 280, coder 282 and uncoder 284, steps are performed to extract OVAN from OBVAN in a manner which is similar to that which was done in block 260, coder 262 and uncoder 264. This extracted OVAN is then applied to a comparator 286 of FIG. 13E, which receives as an additional input the stored OVAN from the check presented by the recipient. If this comparison fails, the process has not been authenticated, and the originator's bank will be notified. On the other hand, if the comparison succeeds, this is an indication that full authentication of the entire process and all parties has occurred and that the message received from the originator's bank is authentic.

Processing then continues by accessing the redeemer's account at block 288, computing a new balance at block 290 and updating the redeemer's account. The redeemer's bank then transmits a message back to the originator's bank, informing it that the redeemer's account has been credited. This information is saved at the originator's bank in temporary storage at block 291. The originator's bank then accesses the originator's account file using his personal account number ORGPAN as an index, and updates his account with the information that was placed in temporary storage at block 273 (FIG. 13D).

The redeemer's bank also communicates with the terminal at which the check was presented (block 294 of FIG. 13D), and informs it that the transaction has been satisfactorily completed and that the recipient may receive payment in the form of cash, goods or services (block 296). The terminal prints the redemption VAN (RDBVAN) on the check.

Although various embodiments of the present invention have been described herein as useful for particular types of transactions, those skilled in the art will appreciate that they actually have universal utility. For example, the last embodiment (depicted in FIGS. 13A-13E) was described as useful in a check transaction system, but it will be appreciated that it would also be useful in a bill payment system as well as a paperless/cashless system (as further described below).

FIGS. 15A, 15B and 15C are functional block diagrams of a credential issuing and authentication system according to an alternate embodiment of the present invention, wherein the alternate embodiment includes many of the features of the embodiments depicted in FIGS. 6-8 and FIGS. 9-12. For example, the alternate embodiment of FIGS. 15A-15C include steps for enrolling an official, enrolling a user, issuing a credential, and authenticating the credential. FIG. 15A illustrates user enrollment, FIG. 15B illustrates issuance of a credential, and FIG. 15C illustrates the authentication of an issued credential. In the alternate embodiment of FIGS. 15A-15C, enrollment of the official is the same as shown in FIG. 9 and, therefore, shall not be discussed further.

Referring to FIG. 15A, a user is enrolled by a previously enrolled official who verifies the user's identity, based on acceptable documentation. Before the user can be enrolled, the official's identity and authority must be authenticated. The official operates a terminal, where he enters his PIN and his TIN, OTIN, and the name code used during his enrollment, which was stored in his File No. 1. OTIN is transmitted to the remote com-

puter, where it is used as an index or address to access the official's File No. 1 and retrieve CPKO (block 1546). CPKO is returned to the terminal.

The official's PIN is applied to irreversible coder 1530, which produces CPNO. CPNO is applied as the key input to an uncoder 1532, which receives CPKO as a data input from the remote computer, and which uncodes CPKO to generate PKO. CPKO is also applied as a key input to a coder 1534, which receives PKO as an input. The coder 1534 codes PKO using CPKO as the key input to generate a coded number for the official (CNO), which represents coded authentication information. Another coder 1538 codes the official's name code using CNO as a key input to generate a coded name code. A mixer 1536 mixes the coded name code, PKO, and CNO and transmits the mixed signal to the sorter 1540 at the remote computer over preferably a secure link.

At the remote computer, the signal transmitted from mixer 1536 is received by the sorter 1540, which separates out PKO, CNO, and the coded name code. PKO is applied as an index (or address) to access the official's File No. 2 and to thereby retrieve CNO, which was previously stored in the official's File No. 2 during the enrollment of the official (see FIG. 9). The CNO transmitted from the terminal and the CNO retrieved from File No. 2 are then compared in a comparator 1542. If the comparison fails, the identity of the official is not authenticated and the enrollment of the user is aborted.

Assuming that the comparison is successful, the comparator 1542 is enabled and sends a signal to an uncoder 1544. The uncoder 1544 then uncodes the coded name code using the CNO retrieved from the official's File No. 2 to regenerate the name code. The name code also accessed from File No. 1 and then compared at 1550. If the comparison fails, the identity of the official is not authenticated and the enrollment of the user is aborted. Assuming that the comparison is successful, the comparator 1550 sends an authentication signal ("okay to enroll user") and user enrollment begins. It should be noted that the "okay to enroll user" signal is applied as a write enabled to the official's File No. 2 at 1552 to save a joint key JKU therein (described below).

At the remote computer, number generator 1516 generates a unique random number (as discussed above), which is assigned to the user as a secret predetermined address or key, PKU. PKU is transmitted over a secured link to the enrollment terminal, where it is applied to the data input of a coder 1504.

The user operates a terminal and selects a PIN which he enters along with his TIN, UTIN. The user's PIN is applied to irreversible coder 1502 which produces the user's coded PIN, CPNU. CPNU is applied as a key input to coder 1504. The output of the coder 1504 is the user's coded predetermined address or key, CPKU. CPKU may be stored in a user record (at block 1510). A mixer 1506 mixes CPNU and CPKU and transmits the mixed signal to the remote CPU.

At the remote computer, sorter 1512 separates the received signal into its component parts CPKU and CPN. At the remote computer, a random number RN is generated (as discussed above) and applied as a key input to coder 1518. The coder 1518 also receives CPN as an input and thereby generates a revisable owner code (ROC). ROC is stored in the user's File No. 1 (at block 1520), wherein the user's File No. 1 is accessed (or addressed) using UTIN. CPKU is also stored in the user's File No. 1 (at block 1520).

PKU is applied as an index or address to the user's File No. 2 in order to store RN (at block 1522). PKU is secret in the system and, therefore, the location and contents of the user's File No. 2 (including RN) is secret. Additional information may be coded in a coder 1524 using CPKU as a key input to generate coded information which is also stored in the user's File No. 2. The information which is coded using CPKU in the coder 1524 may include the secret information RN.

PKU is applied as an input to coder 1528, which also receives CPKO as a key input. The coder 1528 generates a user joint key (JKU) which is stored in the user's File No. 2. JKU is also stored in the official's File No. 2 (at block 1552).

It should be noted that the storage and handling of RN and ROC in the embodiment shown in FIG. 15A is different from the storage and handling of RN and ROC shown in FIG. 6. In FIG. 6, the file in which RN and ROC are stored is generally non-secret because it is indexed (or addressed) by generally non-secret user information (such as the user's TIN). However, in the embodiment shown in FIG. 15A, the non-secret ROC is stored in the user's File No. 1, which is non-secret, and the secret RN is stored in the user's File No. 2, which is secret (since it is accessed or addressed using the secret PKU). Therefore, the embodiment of 15A includes an additional level of security and protection over the embodiment shown in FIG. 6.

FIG. 15B illustrates issuance of a credential according to the alternate embodiment of the present invention. The issuance of credential in the alternate embodiment is essentially the same as the issuance of credentials in the previous embodiment shown in FIG. 11. Note, however, that it is possible to record the ROC retrieved from the user File No. 1 on the credential 1564 since the ROC is public (although the ROC could also have been recorded on the credential in the previous embodiment).

FIG. 15C illustrates the authentication of an issued credential. This is preferably performed at a terminal provided for that purpose. The terminal includes a reading device for the credential 1564 and an input device, such as a keypad, for the user. The information from the credential 1564 could, however, be keyed in by hand. The terminal communicates with the remote processor via a preferably secured link. As part of the credential authentication process, the identity of the user is authenticated. Specifically, the user enters his PIN which is applied as an input to irreversible coder 1570, which generates a coded PIN (CPNU). The user also enters his TIN (UTIN), which is used to access the user File No. 1 (at block 1588) and retrieve CPKU, which is transmitted from the remote CPU to the terminal. CPKU is applied as an input to coder 1574, which also receives CPNU as a key input. The coder 1574 generates a coded number CNU, which represents coded authentication information. CPKU is also applied as an input to uncoder 1572, which also receives CPNU as a key input. The uncoder 1572 uncodes CPKU to regenerate PKU. Both CNU and PKU are mixed by mixer 1576 and sent to the sorter 1578 at the remote CPU.

At the remote CPU, the sorter 1578 separates the signal into its component parts PKU and CNU. PKU is applied as an index into the user's File No. 2 in order to retrieve the secret information RN. UTIN is applied as an index to the user's File No. 1 to retrieve the non-secret revisable owner code (ROC). ROC is applied as an input to uncoder 1584, and the secret information

RN is applied as a key input to uncoder 1584. The uncoder 1584 thereby uncodes ROC using RN in order to regenerate CPNU as RCPN, which is applied as a key input at coder 1582. CPKU, which is read from the credential 1564, is applied as an input to coder 1582. The coder 1582 codes CPKU using RCPN as a key input in order to generate a coded number CNU. The generated coded number CNU is compared at the comparator 1580 to the coded number CNU received from the terminal. If the comparison fails, authentication of the user aborts. However, if the comparison is successful, the user is authenticated and the process continues by authenticating the credential 1564.

The credential 1564 is authenticated by reading the official's ID number OTIN from the credential and using OTIN as an index in order to access the official's File No. 1 and read CPKO (block 1599). CPKO is applied as an input to coder 1598 which also receives PKU as a key input. The coder 1598 codes CPKO using PKU in order to regenerate the user joint key JKU. JKU is also read from the user's File No. 2 using PKU as an index and then applied to a comparator 1596. The comparator 1596 compares the JKU which was retrieved from the user's File No. 2 and the JKU which was generated by the coder 1598. If the comparison fails, then authentication of the credential aborts. However, if the comparison is successful, the comparator 1596 is enabled and sends an okay signal to a comparator 1594.

The JKU retrieved from the user's File No. 2 at 1586 is applied to an uncoder 1592, which also receives as an input the VAN which was read from the credential 1564. The uncoder 1592 uncodes the VAN in order to regenerate INFO. The regenerated INFO is applied as an input to the comparator 1594, which also receives the INFO read from the credential 1564. The comparator 1594 compares the regenerated INFO and the INFO from the credential and if the comparison is successful, the credential is authenticated. Otherwise, the credential is not authenticated.

As noted above, in FIG. 15C, the transmission link between the mixer 1576 and the sorter 1578 is preferably secured since using an unsecured link would present a potential security problem. For example, the signal from the mixer 1576 could be recorded and then transmitted to the sorter 1578 at a later date in order to attempt to fraudulently authenticate a user and a credential. In accordance with an alternate embodiment of the present invention, an anti-duplication variable authentication number (ADVAN) is generated at the terminal by coding at least a transmission date and a time with the CPNU. The ADVAN is then mixed with the CNU and the PKU at the mixer 1576 and sent to the sorter 1578 at the remote CPU over an unsecured link. At the remote CPU, the received ADVAN is uncoded using the derived RCPN to regenerate the transmission date and the time. The regenerated transmission date and time are then compared to a reception date and time (that is, the date and time at which the signal was received at the sorter 1578) and if the comparison is successful, the information transmitted over the transmission medium between the mixer 1576 and the sorter 1578 is authenticated. In this manner, the user and credential are further authenticated.

Alternatively, a semi-random number (not shown) is generated at the terminal using a counter or other random number generator (not shown). The semi-random number is coded using the CPNU to generate a coded semi-random number. The coded semi-random number

is then transmitted along with CNU and PKU to the remote CPU over an unsecured medium. At the remote CPU, the coded semi-random number is uncoded using RCPN to regenerate the semi-random number. A second semi-random number is then generated at the remote CPU using another counter or random number generator (not shown) which is generally synchronized with the counter (not shown) at the terminal. The communication medium between the mixer 1576 and the sorter 1578 is then authenticated by comparing at the remote CPU the regenerated semi-random number to the second semi-random number which was generated at the remote CPU. If the comparison is successful, then the information transmitted over the communication medium between the mixer 1576 and the sorter 1578 is authenticated. In this manner, the user and credential are further authenticated.

As described above, the predetermined secret address PKU is coded to generate the coded secret address CPKU. According to an alternate embodiment, PKU comprises one or more components which are combinable to form the predetermined secret address PKU. In this alternative embodiment, only one of the components of the PKU is transmitted from the remote CPU to the terminal. The coder 1504 (FIG. 15A) codes this one component of the PKU to generate CPKU. Therefore, in this alternate embodiment, CPKU represents a coded portion of the PKU. Then, to access the user's File No. 2, the CPKU is uncoded as described above to regenerate the portion of the PKU. This PKU portion is combined with the other portions of the PKU to regenerate the PKU, which is then used to access the user's File No. 2. The other portions of the PKU may be stored throughout the system, such as in the operating system, in the executive program, in files, etc.

FIG. 16 is a functional block diagram of a system for authenticating the identity of a party and for authorizing access to a party's hidden (or secret) file according to an alternate embodiment of the present invention. The party's hidden file (such as hidden memory file 1622) may contain coded or uncoded secret information. In the embodiment of FIG. 16, the party is in possession of a portable storage media, such as a card 1602 having a magnetic stripe for recording information thereon. The card 1602 is issued by an agency, or a bank, during enrollment of the party. Information recorded on the card 1602 includes the party's revisable owner code (ROC), a coded address (CPK) of the hidden file 1622, an agency identification number (AID or Agency ID), and a transaction sequence number (TSN). The party's ROC is generated as described above (see FIG. 6). The coded address CPK of the hidden memory file 1622 may either represent the entire address of the hidden memory file 1622 or only a portion of the address of the hidden memory file 1622, as described above.

The party to be authenticated enters a personal identification number (PIN) at a terminal. The PIN is input to an irreversible coder 1606 to produce a coded personal identification number (CPN). The information recorded on the party's card 1602 is read from the card 1602 using an appropriate reader (not shown). The CPK read from the card 1602 is applied as an input to an uncoder 1612, which also receives the CPN as a key input. The uncoder 1612 uncodes CPK using CPN as a key input to generate PK, which represents either the total address of the hidden memory file 1622 or a por-

tion of the address of the hidden memory file 1622 (as noted above).

The transaction sequence number (TSN) read from the card 1602 is input to a mixer 1608 and then to a coder 1610. The coder 1610 also receives the CPN as a key input. The coder 1610 codes the TSN using the CPN as a key input to generate an anti-duplication VAN (ADVAN). The ADVAN, PK, ROC, and AID are input to a mixer 1614 and the resulting mixed signal is sent to the remote CPU over a preferably unsecured communication link.

The user's hidden memory file 1622 is part of a memory which is used to store such files at the remote CPU. The sorter 1616 separates the received mixed signal into its component parts ROC, PK, AID, and ADVAN. Where the PK generated by the uncoder 1612 is only a portion of the address to the hidden memory file 1622, the AID is used as an index to a memory table 1618 to retrieve other address components for the hidden memory file 1622. Thus, the address components in the memory table 1618 applicable in any given transaction depends on the particular AID. The PK is combined with the other address components at a combiner 1620 to thereby form the composite address of the hidden memory file 1622. The AID could also identify a predetermined procedure for combining the applicable address components. The composite address is used to access the hidden memory file 1622 to retrieve a secret random number RN (which is generated according to the method described above with respect to FIG. 6). RN is input as a key to a coder 1624. The coder 1624 also receives the ROC from the sorter 1616 and thereby generates CPN.

A transaction sequence number (TSN) is also retrieved from the hidden memory file 1622 and is input to a coder 1632. The coder 1632 also receives CPN as a key input and thereby generates an ADVAN. The ADVAN generated by the coder 1632 is compared with the ADVAN output from the sorter 1616 at a comparator 1630. If a favorable comparison is obtained, then coder 1628 is enabled. If the comparison is not favorable, then the user is not authenticated and does not gain access to the memory file 1622.

Coder 1628 receives PK as an input and CPN as a key and thereby generates CPK. The CPK generated by the coder 1628 is received by an uncoder 1626 as a key input. The uncoder 1626 also receives as input coded information which is retrieved from the hidden memory file 1622. The uncoder 1626 uncodes the coded information from the hidden memory file 1622 using the CPK as a key input to thereby produce clear information. The clear information is then provided to the authenticated user.

As a result of the favorable comparison of the ADVANs at the comparator 1630, a new (or revised) transaction sequence number (TSN) is generated and stored in the hidden memory file 1622. Also, a coder 1634 is enabled. The coder 1634 receives the CPN as an input and also receives a revised RN as a key input. The output of coder 1634 is a new ROC, which is combined with the new TSN in mixer 1635. The mixer 1635 output is sent back to the terminal where the sorter 1604 separates the new TSN and ROC, which are then recorded on the user's card (in order to prepare for the next transaction by the user). Note also that a new CPK may be generated as well by revising a memory address component, such as the address displacement. In this event, the

new CPK would also be returned to the terminal to be recorded on the user's card.

It should be noted that an unsecured communication link between the mixer 1614 and the sorter 1616 is utilized if the hidden memory file 1622 is remote from the location where the party's PIN is entered (that is, the terminal). It should also be noted that the transaction sequence number (TSN), in conjunction with the ADVAN, serves to protect the authenticity of the transaction and the user's card against fraudulent duplication of the transaction information (that is, by recording the output of the mixer 1614 and retransmitting it later to the sorter 1616).

A number of additional applications for the present invention will now be described.

The invention could be utilized in a pay telephone system in which calls could be made without the use of money. The call originator uses a telephone in the usual way to enter the telephone number of the party to be called (i.e., to the call recipient). The call originator also enters his own telephone number and PIN. The system then authenticates the identity of the originator as described above (by using, for example, the embodiment depicted in FIGS. 6-8 or in FIGS. 9-12). In the first embodiment (i.e., FIGS. 6, 7, 8A and 8B), the originator's PIN is coded, and used to derive an arbitrary number, which is subsequently compared to another such number which is generated from a reconstituted version of the coded PIN. The reconstituted coded PIN is formed from an RN and ROC which are accessed from the originator's account file, with the originator's telephone number serving as a file index. If the comparison is unfavorable, the call is aborted; otherwise, call processing continues.

In the second embodiment, the originator's telephone number is used as an index to file no. 1 to access an originator's CPKO and true CNO. The originator's coded PIN, CPNO, is then combined with the originator's CPKO to generate a CNO (as in FIG. 12). The originator's identity is then authenticated by comparing the true CNO with the derived CNO. If the comparison is unfavorable, the call is aborted; otherwise, processing continues. The originator can use a machine readable card, or the like which has CPKO and CNO previously recorded thereon. In this event, access to file no. 1 is unnecessary.

In either embodiment, if the identity comparison is favorable, then the originator's credit balance is extracted from the originator's file to determine whether the call should be allowed. If the credit balance is favorable, then the telephone connection is extended to the call recipient, and the recipient's telephone is rung.

At the end of the call, the originator's credit balance is diminished by the cost of the call, and the new balance is computed and rewritten to the originator's file. The originator may then be advised of the cost of the call. When the recipient's telephone rings and the call is answered, the system can require that the identity of the person answering the phone be authenticated, as in a person to person call. In this event, the recipient is asked to enter a PIN, and the recipient's identity is authenticated using either of the two embodiments mentioned above.

Alternatively, a first joint code could be generated when the call is initiated, e.g., from the originator's CPN, and the recipient's reconstituted CPN. When the call is answered, the recipient enters his PIN, which is converted to a CPN and combined with the originator's

reconstituted CPN to form a second joint code. A comparison then ensues between the first and second joint codes.

Another application of the invention is a system which uses a bill as the means of (or vehicle for) payment. The bill contains the usual payment information, and a VAN is also recorded on the bill when the bill is generated. The VAN is derived from the payment information (INFO) and identification information associated with the originator of the bill (e.g., similar to the bank identification line of information which appears at the bottom of an originator's check) or the originator's TIN and BIN. The bill may also contain the recipient's TIN and BIN. Preferably, the above information is coded in a standard format, at a fixed location on the bill itself. The bill is then used in an appropriate document reader to provide the transaction payment information to the system. The party paying the bill (i.e., the payor) enters his PIN and the payor is then authenticated using the PIN. Also, the VAN is authenticated (using one of the methods described above). If the payor and the VAN are authentic, the bill is paid. A redemption VAN is generated (using information associated with the payee party) and printed on the bill, when it has been paid.

Alternatively, the payor could simply key in the information from the face of the bill. When the transaction is completed, a redemption VAN is displayed to the payor, which he records on the bill (or the VAN could be automatically recorded on the bill).

In accordance with a further application of the embodiments of this invention, a medical prescription form which has been originated and issued by a doctor to a patient (a recipient), can be authenticated to permit dispensing of the designated medicine, or drug, in a processing jurisdiction, along with automated payment. Automated payment may include a third party such as an insurance provider. This system is particularly useful for a patient who is in desperate need of medicine, and is in a remote or strange environment, where the prescription cannot be easily authenticated, or an available pharmacy cannot be found.

The prescription form contains identification information associated with the doctor and the patient, and the usual information which appears on a prescription, such as the type of medicine, strength, quantity, application, date, refills, generic, and a control number. The prescription form also contains a VAN, which is the result of coding the medical and identification information. Preferably, the information and the VAN are recorded on the prescription form so that it is readable by an individual, and it also includes coded symbols or characters representing the same information in machine readable form.

When the prescription form is utilized by the recipient to obtain the medicine from a processing entity (such as a drug store), the information on the form is read automatically by a terminal of the system, or it is entered via a keyboard. The recipient also enters his PIN, and the system authenticates the prescription form, the doctor, and the recipient in accordance with the embodiments described previously. An indication of the cost of the prescribed medicine, and the method of payment is provided to the recipient. The recipient may elect to pay by using one of the methods described herein.

Note that the processing entity may also include a centralized clearinghouse in communication with dis-

persing outlets (i.e., drug stores) for authenticating prescriptions. An RVAN may be generated from the VAN and information associated with the processing entity, and then associated with the transaction, to thereby document the processing entity's involvement in the transaction.

If a patient attempts to use a prescription in a state where the originating physician is not licensed, such as out of state, the original prescription may not be usable. In this situation, a directory system of predetermined licensed "correspondent" physicians may be established, and a correspondent physician can automatically authorize the prescription of an originating physician (on-line), after the original prescription is authenticated.

The invention also finds utility in a paperless/cashless transaction system, in which "funds transfer" transactions, such as purchases, occur without the use of money, or checks. In this system, the payment originator uses a payment recipient's terminal which stores information to identify the precise location of the recipient's account. Alternatively, an originator PIN, information identifying an originator account and a recipient account, and funds transfer information (INFO) which includes a payment amount are entered directly into a terminal of this system by the payment originator. The system initially generates a VAN, (OVAN), by using the payment information (INFO) in conjunction with the identification information associated with the payment originator and payment recipient. The payment originator is authenticated using the originator PIN using a method described above. The system then approves or disapproves the payment based upon an authentication of the VAN, and the "joint" identification information associated with the participants, and the availability of funds, or credit. Such transactions are carried on entirely electronically, the participant's bank accounts are credited and debited automatically, allowing commercial transactions to be completed "instantaneously". An RVAN may be generated using the INFO and printed on a receipt which is dispensed to the originator.

Although preferred embodiments of the invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that many additions, modifications, and substitutions are possible without departing from the scope or spirit of the invention as defined in the accompanying claims.

I claim:

1. In a system comprising a first storage means addressable using a secret predetermined address and party information associated with a party and stored in the first storage means, the party information comprising first coded authentication information previously generated by using a personal identification number (PIN) associated with the party, a method for authenticating the party comprising the steps of:

- (a) receiving a (PIN) from the party to be authenticated;
- (b) addressing the first storage means using the secret predetermined address to locate the party information and to retrieve the first coded authentication information;
- (c) generating second coded authentication information using the received PIN;
- (d) comparing at least part of the retrieved first coded authentication information to at least part of the generated second coded authentication information; and

(e) authenticating the party if said at least part of the retrieved first coded authentication information corresponds to said at least part of the generated second coded authentication information;

wherein the step of addressing the first storage means comprises the steps of:

(1) accessing a second storage means using a non-secret predetermined address to locate and to retrieve a coded address previously stored in the second storage means, the coded address having been previously generated by coding the secret predetermined address of the first storage means using the PIN;

(2) uncoding the coded address using the received PIN to generate the secret predetermined address; and

(3) accessing the first storage means using the generated secret predetermined address to retrieve the first coded authentication information.

2. The method of claim 1, wherein the coded address is extracted from a storage means which is in the possession of the party.

3. The method of claim 1, wherein the first storage means is a part of a memory and wherein, prior to use of the memory, pseudo information is stored in the memory, thereby making unused portions of the memory indistinguishable from the first storage means.

4. The method of claim 1, wherein the party information also comprises secret information associated with the party.

5. A method for enrolling and authenticating a party, comprising the steps of:

receiving a personal identification number (PIN) from the party;

generating coded authentication information using the received PIN;

generating first and second numbers such that the coded authentication information is derivable from the first and second numbers, the first number being secret and the second number being non-secret;

storing information comprising the secret number in a first storage means addressable using a predetermined secret address;

generating a coded secret address using at least part of the predetermined secret address and the received PIN; and

storing the coded secret address and the non-secret number in a second storage means addressable using a predetermined non-secret address.

6. The method of claim 5, wherein the step of storing the information comprising the secret number in the first storage means comprises the steps of:

coding the information comprising the secret number using non-secret information associated with the party to generate coded information; and storing the coded information in the first storage means.

7. The method of claim 6, wherein the non-secret information associated with the party is the coded secret address.

8. The method of claim 5, further comprising the steps of:

receiving a second PIN from a party to be authenticated;

generating at a first site second coded authentication information using the received second PIN;

27

addressing the second storage means using the predetermined non-secret address to locate and retrieve the coded secret address and the non-secret number;

generating at the first site a first coded number using the second coded authentication information and the coded secret address;

generating the predetermined secret address using at least the received second PIN and the retrieved coded secret address;

transmitting at least the first coded number and the predetermined secret address from the first site to a second site;

addressing the first storage means using the generated predetermined secret address to locate and retrieve the secret number;

deriving at the second site the first coded authentication information using the retrieved non-secret number and the retrieved secret number;

generating at the second site a second coded number using the derived first coded authentication information and the coded secret address; and

authenticating the party to be authenticated if the first coded number corresponds to the second coded number.

9. The method of claim 8, further comprising the step of generating at the first site an anti-duplication variable authentication number (ADVAN) by coding at least a transmission date and time with the second coded authentication information, the transmitting step comprising the step of transmitting the first coded number, the predetermined secret address, and the ADVAN from the first site to the second site via an unsecured communication medium.

10. The method of claim 9, further comprising the steps of:

uncoding the ADVAN at the second site using the derived first coded authentication information to regenerate the transmission date and time; and

further authenticating the party to be authenticated if the regenerated transmission date and time correspond to a reception date and time.

11. The method of claim 8, wherein a first semi-random number is generated at the first site using a first counter, and further comprising the step of coding the first semi-random number to generate a coded first semi-random number, and wherein the transmitting step comprises transmitting the first coded number, the predetermined secret address, and the coded first semi-random number from the first site to the second site via an unsecured communication medium.

12. The method of claim 11, further comprising the steps of:

uncoding the coded first semi-random number at the second site to regenerate the first semi-random number;

generating at the second site a second semi-random number using a second counter which is generally synchronized with the first counter; and

further authenticating the party to be authenticated if the regenerated first semi-random number corresponds to the second semi-random number.

13. The method of claim 8, wherein the predetermined secret address comprises one or more components combinable to form the predetermined secret address, the step of generating the coded secret address comprising the step of coding one of the components of

28

the predetermined secret address using the received first PIN to generate the coded secret address.

14. The method of claim 13, wherein the step of generating the predetermined secret address comprises the steps of:

uncoding the retrieved coded secret address using the received second PIN to generate said one of the components of the predetermined secret address; and

generating the predetermined secret address by combining the generated said one of the components with the other components of the predetermined secret address.

15. A method for authenticating a party and for authorizing access to a storage means associated with the party, the storage means being addressable using a secret predetermined address, the method comprising the steps of:

receiving a personal identification number (PIN) from a party to be authenticated;

generating coded authentication information using the PIN, the coded authentication information being derivable from a secret number previously stored in the storage means and a non-secret number previously stored in a storage medium in possession of the party;

retrieving from the storage medium at least a coded address and the non-secret number, the coded address having been previously generated by coding at least a portion of the secret predetermined address using the coded authentication information;

generating said at least a portion of the secret predetermined address by uncoding the coded address using the coded authentication information;

transmitting at least the generated said at least a portion of the secret predetermined address and the retrieved non-secret number from a first site to a second site over a communication link;

generating at the second site the secret predetermined address using the transmitted said at least a portion of the secret predetermined address;

addressing the storage means using the generated secret predetermined address to retrieve the secret number;

deriving the coded authentication information using the retrieved secret number and the transmitted non-secret number; and

authenticating the party and authorizing further access to the storage means by using at least the derived coded authentication information.

16. The method of claim 15, further comprising the steps of:

retrieving from the storage medium a first transaction sequence number (TSN) previously stored therein;

generating a first anti-duplication variable authentication number (ADVAN) by coding the first TSN with the coded authentication information;

transmitting the first ADVAN from the first site to the second site over the communication link;

addressing the storage means using the generated secret predetermined address to retrieve a second TSN previously stored therein;

generating a second ADVAN by coding the second TSN with the derived coded authentication information; and

authenticating the party and authorizing further access to the storage means if the second ADVAN corresponds to the first ADVAN;

29

wherein the first and second TSNs are modified after each transaction, such that fraudulent receipt and use of messages over the communication link and fraudulent duplication of the storage medium are prevented.

17. The method of claim 15, further comprising the steps of retrieving agency identification information from the storage medium and transmitting the agency identification information from the first site to the second site over the communication link, wherein the step of generating at the second site the secret predetermined address comprises the steps of using the agency identification information to retrieve other portions of the secret predetermined address and combining the transmitted said at least a portion of the secret predetermined address with the other portions to form the secret predetermined address.

18. The method of claim 15, further comprising the step of revising the TSN, the secret number, and/or the coded address.

19. The method of claim 15, wherein the communication link is unsecured.

20. A system for authenticating a party comprising:
means for receiving a personal identification number (PIN) from the party;
means for generating coded authentication information using the received PIN;
means for generating first and second numbers such that the coded authentication information is derivable from the first and second numbers, the first number being secret and the second number being non-secret;
means for storing the secret number in a first storage means addressable using a predetermined secret address;

30

means for generating a coded secret address using at least a part of the predetermined secret address and the received PIN; and

means for storing the coded secret address and the non-secret number in a second storage means addressable using a predetermined non-secret address.

21. The system of claim 20, wherein the second storage means is a storage medium in the possession of the party.

22. In a system comprising a storage means addressable using a secret predetermined address and a first coded number previously stored in the storage means and derivable from the secret predetermined address and a coded address generated by coding the secret predetermined address with first coded authentication information associated with a party to be authenticated, a method for authenticating the party comprising the steps of:

receiving a PIN from the party to be authenticated;
generating second coded authentication information using the received PIN;
deriving the secret predetermined address by uncoding the coded address using the second coded authentication information;
generating a second coded number by coding the derived secret predetermined address with the coded address;
using the derived secret predetermined address to access the storage means and retrieve the first coded number; and
authenticating the party if the retrieved first coded number corresponds to the generated second coded number.

* * * * *

United States Patent [19]

Rivest et al.

[11] 4,405,829

[45] Sep. 20, 1983

[54] CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD

[75] Inventors: Ronald L. Rivest, Belmont; Adi Shamir, Cambridge; Leonard M. Adleman, Arlington, all of Mass.

[73] Assignee: Massachusetts Institute of Technology, Cambridge, Mass.

[21] Appl. No.: 860,586

[22] Filed: Dec. 14, 1977

[51] Int. Cl.³ H04K 1/00; H04I 9/04

[52] U.S. Cl. 178/22.1; 178/22.11

[58] Field of Search 178/22, 22.1, 22.11, 178/22.14, 22.15

[56] References Cited

U.S. PATENT DOCUMENTS

3,657,476 4/1972 Aiken 178/22

OTHER PUBLICATIONS

"New Directions in Cryptography", Diffie et al., *IEEE Transactions on Information Theory*, vol. IT-22, No. 6, Nov. 1976, pp. 644-654.

"Theory of Numbers" Stewart, MacMillan Co., 1952, pp. 133-135.

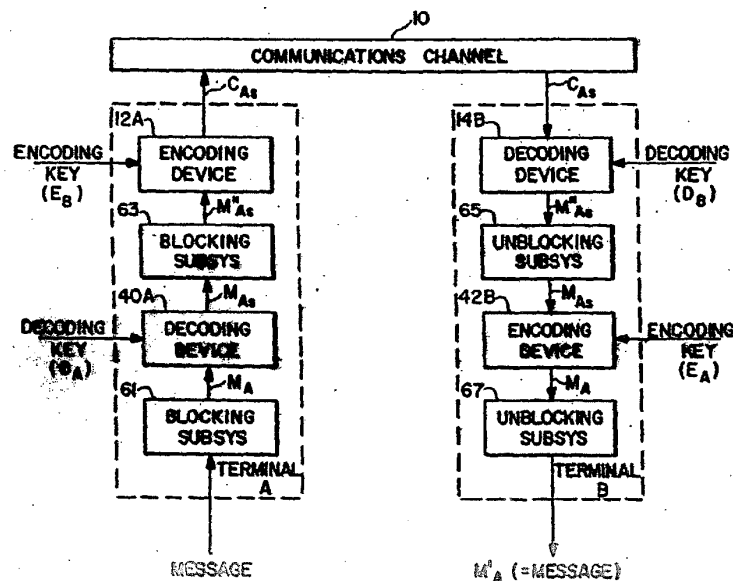
"Diffie et al., Multi-User Cryptographic Techniques", AFIPS Conference Proceedings, vol. 45, pp. 109-112, Jun. 8, 1976.

Primary Examiner—Sal Cangialosi
Attorney, Agent, or Firm—Arthur A. Smith, Jr.; Robert J. Horn, Jr.

[57] ABSTRACT

A cryptographic communications system and method. The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to ciphertext at the encoding terminal by first encoding the message as a number M in a predetermined set, and then raising that number to a first predetermined power (associated with the intended receiver) and finally computing the remainder, or residue, C , when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver). The residue C is the ciphertext. The ciphertext is deciphered to the original message at the decoding terminal in a similar manner by raising the ciphertext to a second predetermined power (associated with the intended receiver), and then computing the residue, M' , when the exponentiated ciphertext is divided by the product of the two predetermined prime numbers associated with the intended receiver. The residue M' corresponds to the original encoded message M .

40 Claims, 7 Drawing Figures



STAM0041681

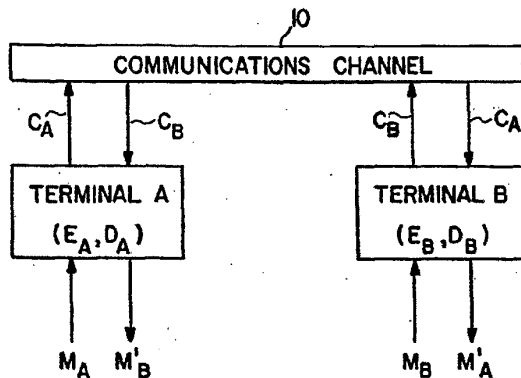


FIG. 1

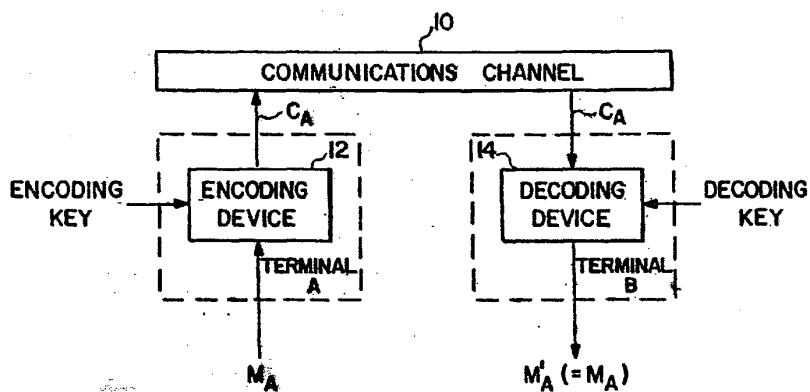


FIG. 2

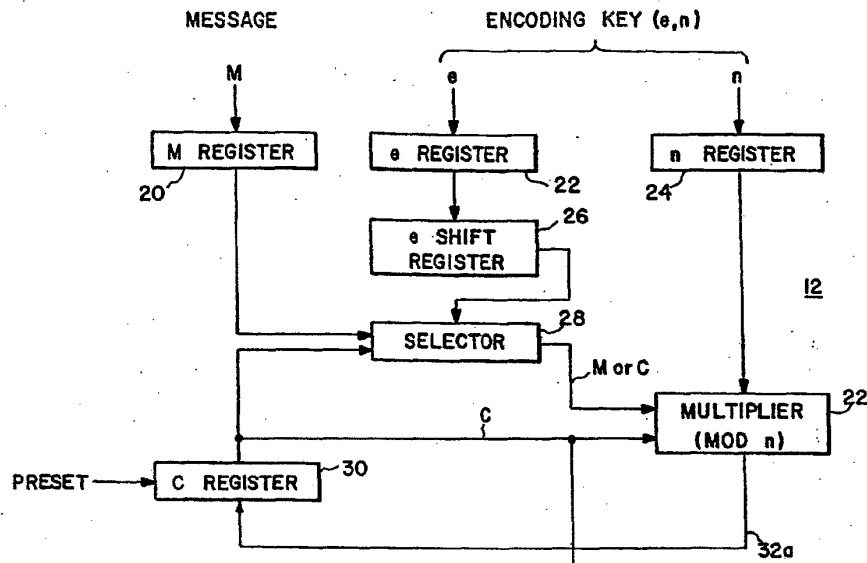


FIG. 3 CIPHER TEXT C

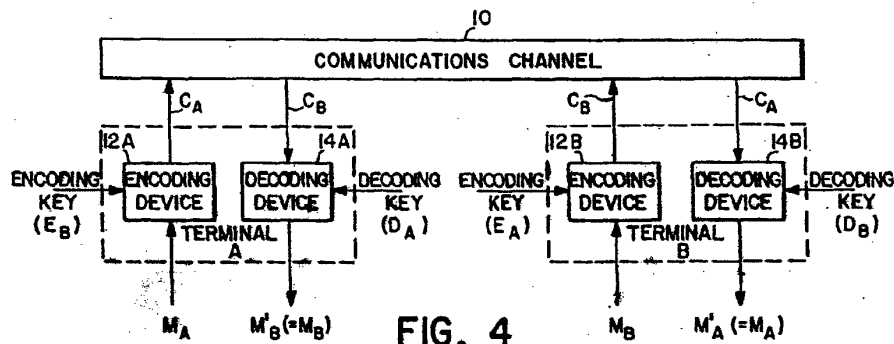


FIG. 4

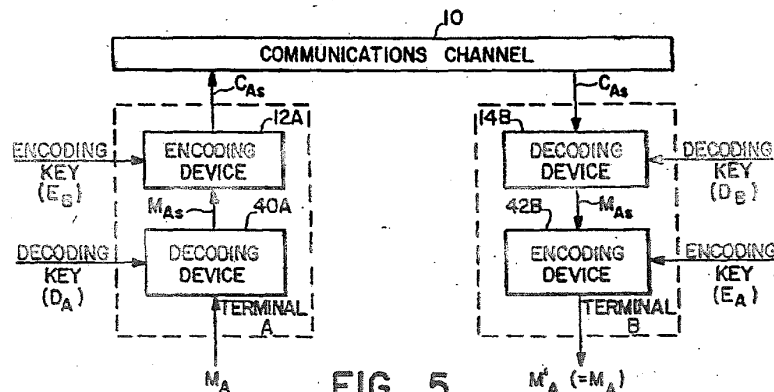


FIG. 5

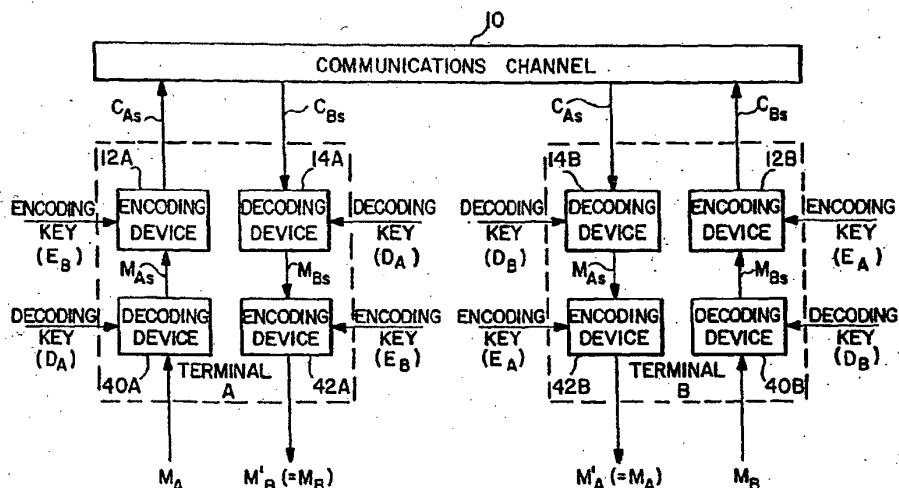


FIG. 6

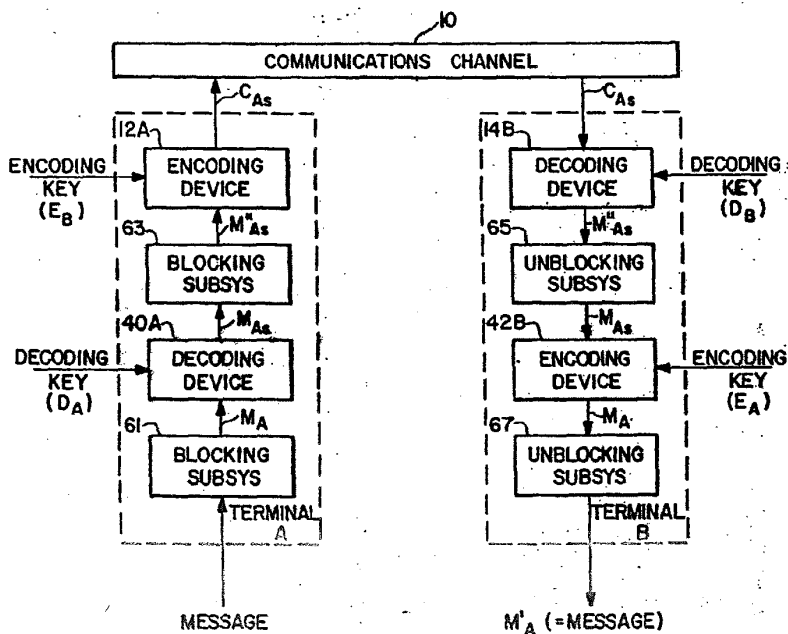


FIG. 7

CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD

The Government has rights in this invention pursuant to Contract No. N00014-67-A-0204, awarded by the Department of the Navy, and Grant No. MCS76-14249, awarded by the National Science Foundation.

BACKGROUND OF THE DISCLOSURE

This invention relates to communications, and more particularly to cryptographic communications systems and methods.

With the development of computer technology, the transfer of information in digital form has rapidly increased. There are many applications, including electronic mail systems, bank systems and data processing systems, where the transferred information must pass over communications channels which may be monitored by electronic eavesdroppers. While the degree of security required may vary for various applications, it is generally important for all of these examples that the substance of particular communications pass directly from a sender to an intended receiver without intermediate parties being able to interpret the transferred message. In addition, there are further instances where information in computer memory banks must be protected from snoopers who have access to the memory through data processing networks.

In addition to these privacy requirements, authentication of the source of a message must often be insured along with the verification and security of the message content. For example, in banking applications, it is required that a signed document, such as a bank draft, be authenticated as being actually signed by the indicated signator. Furthermore, in many applications, it is desirable to further require safeguards against signature forgery by a message recipient.

In the prior art, a number of cryptographic encoding and decoding techniques are readily available to provide some degree of privacy and authentication for digital communications, for example, the data encryption standards adopted by the National Bureau of Standards, see *Federal Register*, Mar. 17, 1975, Volume 40, No. 52 and Aug. 1, 1975, Volume 40, No. 149.

In general, cryptographic systems are adapted to transfer a message between remote locations. Such systems include at least one encoding device at a first location and at least one decoding device at a second location, with the encoding and decoding devices all being coupled to a communication channel. For digital systems, the message is defined to be a digital message, M , that is, a sequence of symbols from some alphabet. In practice, the alphabet is generally chosen to be the binary alphabet consisting of the symbols 0 and 1.

Each encoding device is an apparatus which accepts two inputs: a message-to-be-encoded, M , and an encoding key or operator, E . Each encoding device transforms the message M in accordance with the encryption operator to produce an encoded version C of the message (which is denoted as the ciphertext) where $C=E(M)$. The encoding key and the ciphertext are also digital sequences.

Each decoding device is an apparatus which accepts two inputs: a ciphertext-to-be-decoded C and a decoding key or operator, D . Each decoding device transforms the ciphertext in accordance with the decryption operator to produce a decoded version M' of the cipher-

text where $M'=D(C)$, or $M'=D(E(M))$. Like the encoding key, the decoding key and decoded message M' are also digital sequences. The encoding and decoding keys are selected so that $M'=M$ for all messages M .

In operation, a message, once encoded into ciphertext, is transmitted over the channel to a recipient who decodes the received ciphertext to obtain the original message M . Thus, a recipient sees the original message M as the output of his decoding device.

To a large degree, the quality of performance of a cryptographic system depends on the complexity of the encoding and decoding devices. Regarding the problem of ensuring privacy of communications for a system where an eavesdropper can listen to every message transmitted on the communications channel (which might, for example, be a radio link), the effectiveness of the system depends upon the ability to ensure that the eavesdropper is unable to understand any such overheard messages. In the prior art systems, the sender and recipient arrange to have corresponding encoding and decoding keys which are kept secret from the eavesdropper, so that even if the eavesdropper knows the construction of the encoding and decoding devices, he would not be able to decode the messages he hears, even after hearing a large number of messages. In practice, however, this constraint results in extremely complex and correspondingly expensive equipment. A disadvantage of the prior art systems results from the general requirement that the pre-arranged encoding and decoding keys must be delivered in a secure fashion (often by courier) to the sender and receiver, respectively, to enable communication through the systems.

The "public-key cryptosystem" described by Diffie and Hellman, "New Directions In Cryptography", IEEE Transactions on Information Theory (Nov. 1976), in principle, provides enciphered communication between arbitrary pairs of people, without the necessity of their agreeing on an enciphering key beforehand. The Diffie and Hellman system also provides a way of creating for a digitized document a recognizable, unforgeable, document-dependent, digitized signature whose authenticity the signer cannot later deny.

In a public-key cryptosystem, each user (e.g. user A) places in a public file an enciphering operator; or key, E_A . User A keeps to himself the details of the corresponding deciphering key D_A which satisfies the equation

$$D_A(E_A(M))=M.$$

for any message M . In order for the public key system to be practical, both E_A and D_A must be efficiently computable. Furthermore, user A must not compromise D_A when revealing E_A . That is, it should not be computationally feasible for an eavesdropper to find an efficient way of computing D_A , given only a specification of the enciphering key E_A (even though a very inefficient way exists: to compute $D_A(C)$, just enumerate all possible messages M until one such that $E_A(M)=C$ is found. Then $D_A(C)=M$). In a public key system, a judicious selection of keys ensures that only user A is able to compute D_A efficiently.

Whenever another user (e.g. user B) wishes to send a message M to A, he looks up E_A in the public file and then sends the enciphered message $E_A(M)$ to user A. User A decipheres the message by computing D_A . ($E_A(M))=M$. Since D_A is not derivable from E_A in a practical way, only user A can decipher the message

$E_A(M)$ sent to him. If user A wants to send a response to user B, user A enciphers the message using user B's encryption key E_B , also available in the public file. Therefore no transactions between users A and B, such as exchange of secret keys, are required to initiate private communication. The only "setup" required is that each user who wishes to receive private communication must place his enciphering key E in the public file.

The public key approach of Diffie and Hellman is also useful in principle to provide signed digital messages that are both message-dependent and signer-dependent. The recipient of a "signed" message not only knows the message substance, but also can provide that the message originated from the identified sender. A signed message precludes the possibility that a recipient could modify the received message by changing a few characters or that the recipient could attach the received signature to any message whatsoever. This is a particular problem for digital messages inasmuch as electronic "cutting and pasting" of sequences of characters are generally undetectable in the final product.

In order to implement signatures on messages transferred between two users, e.g. user A and user B, in accordance with the Diffie and Hellman system, each user has encoding keys E_A and E_B , respectively, on a public file and decoding keys D_A and D_B , respectively, privately held. Each user's encoding and decoding keys must effect permutations of the same message space S, so that the following relations hold:

$$D_A(E_A(M)) = M$$

$$E_A(D_A(M)) = M$$

$$D_B(E_B(M)) = M$$

$$E_B(D_B(M)) = M$$

for any message M.

When user A wants to send user B a "signed" document M, user A first uses his own decryption key D_A to transform M into a signed message word $M_s = D_A(M)$. User A then uses user B's encryption key E_B (from the public file) to generate a signed ciphertext word $C_s = E_B(M_s) = E_B(D_A(M))$, which is sent to user B. User B initially uses his secret decryption key D_B to reduce the signed ciphertext C_s to a signed message word in accordance with $D_B(C_s) = D_B(E_B(M_s)) = M_s$. Now using user A's encoding key E_A (available from the public file), user B decodes the signed message word in accordance with $E_A(M_s) = E_A(M)$.

User A cannot deny having sent user B this message, since no one but A could have created $M_s = D_A(M)$, provided that D_A is not computable from E_A . Furthermore, user B can show that the public key E_A is necessary to extract the message M so that user B has "proof" that user A has signed the document. User B cannot modify M to a different version M', since then user B would have to create the corresponding signature $D_A(M')$ as well. Therefore user B must have received a document "signed" by A, which he can "prove" that A sent, but which B cannot modify in any detail.

While the public-key cryptosystem principles as described above, and their potential use as a means of implementing digital "signatures", are known in the prior art, there are no practical implementations which are known, either with or without signature.

Accordingly, it is an object of this invention to provide a system and method for implementing a private communications system.

It is another object to provide a system and method for establishing a private communications system for transmission of signed messages.

It is still another object to provide a system and method for implementing a public key cryptographic communications system.

It is a further object to provide a system and method for encoding and decoding digital data.

SUMMARY OF THE INVENTION

Briefly, the present invention includes at least one encoding device, at least one decoding device, and a communication channel, where the encoding and decoding devices are coupled to the channel. The encoding device is responsive to an applied message-to-be-transmitted M and an encoding key to provide a ciphertext word C for transmission to a particular decoding device. The encoding key E is a pair of positive integers e and n which are related to the particular decoding device. The message M is a number representative of a message-to-be-transmitted and wherein

$$0 \leq M \leq n-1$$

where n is a composite number of the form

$$n = p \cdot q$$

ps where p and q are prime numbers.

For messages represented by numbers outside the range 0 to n-1, a conventional blocking means is utilized to break the message into message block words before encoding, where each block word is representative of a number within the specified range. Following subsequent decoding, the recovered block words may be transformed back to the original message.

The presently described encoding device can distinctly encode each of the n possible messages. In alternative but equivalent embodiments, the numbers representative of the possible messages-to-be-transmitted need not be integers in the range 0 to n-1, but could be integers selected from each residue class modulo n. For example, where n=3, the numbers representative of the set of messages-to-be-transmitted might include 0(=0 mod 3), 10(=1 mod 3), and 8(=2 mod 3). Accordingly, the range limitations for n expressed hereafter in this application are appropriate for the numbers in the modulo residue classes within the respective ranges, but it will be understood that numbers outside the range but selected from the appropriate residue classes are considered to be equivalent to those within the specified range and are intended to be embraced by the claims.

The transformation provided by the encoding device is described by the relation

$$C = M^e \pmod{n}$$

where e is a number relatively prime to (p-1)(q-1).

The particular decoding device is also coupled to the channel and is adapted to receive the ciphertext C from the channel. The decoding device is responsive to the received ciphertext word C and a decoding key to transform that ciphertext to a received message word M'. The decoding key D is a pair of positive integers d and n. M' is a number representative of a deciphered

5

form of C (i.e. reconstituted plaintext) and corresponds to the relation

$$M' = C^d \pmod{n}$$

where d is a multiplicative inverse of $e \pmod{1, \text{cm}((p-1), (q-1))}$ so that

$$e \cdot d \equiv 1 \pmod{1, \text{cm}((p-1), (q-1))}$$

where $1, \text{cm}((p-1), (q-1))$ is the least common multiple of numbers $p-1$ and $q-1$.

With these encoding and decoding devices, a message sent from the encoding device to the decoding device is transformed from M to C by the encoding device, and then back from C to M' by the decoding device, where $M' = M \pmod{n}$.

In a communication system which is adapted to provide digital signatures, each transmitting and receiving terminal is provided with both an encoding and decoding device, each device being functionally equivalent to the devices described above but operating on a different set of input words with a different key. The transmitting terminal decoding device transforms a message M using its own decoding key to generate a signed message M_s . Then the encoding device transforms the resultant signed message M_s with the intended receiving terminal's encoding key to generate signed ciphertext word C_s . The receiving terminal's decoding device then transforms the received C_s with its own decoding key to obtain the signed message M_s , and then the encoding device transforms the resultant signed message with the transmitting terminal's encoding key to obtain the original message. For example, in a system for transmitting signed messages from user A to user B, the terminal for user A includes at least one encoding device characterized by an encoding key $E_A = (e_A, n_A)$ and at least one decoding device, characterized by a decoding key $D_A = (d_A, n_A)$. Similarly, the terminal for user B includes an encoding device characterized by an encoding key $E_B = (e_B, n_B)$ and a decoding device characterized by a decoding key $D_B = (d_B, n_B)$. The encoding and decoding devices of terminals A and B are of the same form described above for the privacy system.

In operation, to provide a signed message, user A first generates a ciphertext signed message word M_s

$$M_s = M^e \pmod{n_A}$$

and then transforms that signed message word to a signed ciphertext word C_s :

$$C_s = M_s^e \pmod{n_B}$$

which is then transferred to user B. User A may readily use d_A and n_A from his own decoding key to reduce the signed ciphertext word to a signed message word, and then perform the encoding transformations using e_B and n_B from the publicly available file.

User B decipheres the received C_s into the signed message word M_s in accordance with

$$M_s = C_s^{d_B} \pmod{n_B}$$

User B then transforms M_s to M in accordance with

$$M = M_s^{d_A} \pmod{n_A}$$

6

User B may readily perform his decoding transformations since d_B and n_B are part of his decoding key and e_A and n_A are readily available on the public file.

In any of the above operations, the underlying messages may be initially encoded using conventional encryption techniques, and the subsequently decoded messages may be decoded using a corresponding decryption technique. The present invention may be used with any length messages provided that the message is broken into suitable length blocks before encoding. For example, very long messages may readily be broken into blocks, with each block labelled with a "this is block t of R" notation and transmitted after signing each block separately. Any word to be transformed, using either the encoding or decoding key for a terminal, must be broken into blocks, wherein each block is representative of a number in the range 0 to $n-1$ for the corresponding terminal. Following transmission over the channel and the second transformation, the resultant words may readily be "unblocked".

The present invention provides a public key system for establishing private communications and also for providing private communications with the signature. A characteristic of this system is that the public revelation of the encryption key does not reveal the corresponding decryption key. As a result, couriers or other secure means are not required to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only the intended recipient can decipher the message since only he knows the corresponding decryption key. Furthermore, the message can be "signed" by deciphering it with the privately held decryption key. Anyone can verify the signature using the corresponding publicly revealed encryption key corresponding to the originator. Signatures cannot be forged and the signer cannot later deny the validity of his signature.

In other forms, the present invention may be utilized with both the encoding and decoding keys secret. In such forms, if users A and B wish to communicate privately over an insecure channel, they may use the channel to transmit E_A and E_B to B and A, respectively. Then when A wishes to send B a message M, he first produces $E_B(M) = C$ and sends this to B. B applies D_B to C to obtain M. An eavesdropper on the channel will have access to E_B , E_A and C but without access to D_B is unable to decode C.

In alternative forms, the present invention may be utilized with the encoding and decoding devices coupled by a data path to a memory so that encoded only, or encoded signed, data words may be stored in the memory, thereby ensuring file integrity. In such an embodiment, the data path and memory are considered to be a communications channel coupling the encoding and decoding devices (which devices may be at the same physical location). In addition, the present system is suitable for use in access control systems.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects of this invention, the various features thereof, as well as the invention itself, may be more fully understood from the following description, when read together with the accompanying drawings in which:

FIG. 1 shows in block diagram form, a communications system in accordance with the present invention;

FIG. 2 shows in block diagram form an embodiment of the system of FIG. 1 adapted to transfer enciphered

digital messages in one direction between two terminals;

FIG. 3 shows in detailed block diagram form, the encoding device in the system of FIG. 2;

FIG. 4 shows in block diagram form an embodiment of the system of FIG. 1 adapted to transfer enciphered digital messages in two directions between two terminals;

FIG. 5 shows in block diagram form, an embodiment of the system of FIG. 1 adapted to transfer signed, enciphered digital messages in one direction between two terminals;

FIG. 6 shows in block diagram form, an embodiment of the system of FIG. 1 adapted to transfer signed, enciphered digital messages in two directions between two terminals; and

FIG. 7 shows in block diagram form, an embodiment of the system of FIG. 1 adapted to transfer blocked messages in one direction between two terminals.

DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 shows an embodiment of the present invention in block diagram form. This system includes a communications channel 10 and two terminals A and B coupled to the channel, where each terminal has an associated encoding key E and decoding key D: E_A, D_A , respectively, for terminal A and E_B, D_B , respectively, for terminal B. The communications channel 10 may include, for example, a conventional broad-band cable with associated modulator and demodulator equipment at the various remote terminals to permit data transfer between terminals connected to the channel and the channel itself. The system of FIG. 1 is suitable for the two-way transfer of messages between terminal A and terminal B. Each of terminals A and B is adapted to transform a plaintext message to an encoded form and transfer the encoded message over channel 10 to the other terminal. When received at the other terminal, the encoded message is transformed back to its plaintext form. In the figures, the message, encoded form and reconstituted plaintext are represented by the symbols M, C, and M', respectively, with subscripts A or B being representative of the originating terminal.

In one embodiment (e.g. the system of FIG. 2 described below), the encoded form of the message is encrypted to ciphertext that may only be decoded by the intended receiver terminal. In a second embodiment, the encoded form is representative of a message combined with a digital signature indicative of the sending terminal. In a third embodiment (e.g. the system of FIG. 5 described below), the encoded form is both encrypted to a form intelligible only to the intended receiver and also signed by the sending terminal. Alternative form systems may include additional remote terminals (each having associated encoding and decoding keys) coupled to the channel 10, as well as associated terminal and channel equipment so that messages may be addressed to particular ones of the terminals in a conventional manner.

FIG. 2 shows a form of the invention wherein messages M_A may be transferred in encrypted form in one direction from terminal A to terminal B. In this embodiment, terminal A includes an encoding device 12 and terminal B includes a decoding device 14.

Encoding device 12 is adapted to receive an input message M_A to be transferred to the terminal B. Message M_A may be pre-coded by conventional encoding

techniques to a digital form. In embodiments, where relatively large messages are being utilized, the pre-coded form may be in terms of short data blocks which may be individually encoded by the device 12 into corresponding words of ciphertext C_A . To establish communications with terminal B, the encoding device 12 performs the transformation from M_A to C_A utilizing the terminal B encoding key, E_B (defined more fully below). The decoding device 14 receives ciphertext words C_A from the channel 10 and transforms them into reconstituted plaintext from M_A' utilizing the terminal B decoding key, D_B (defined more fully below). The encoding and decoding keys are adapted so that the decoded message M_A' is the same as the message M_A . To establish communication with any other terminal, the encoding device 12 of the sending terminal utilizes the encoding key associated with the intended receiver terminal. The decoding device 14 of the receiving terminal utilizes its own decoding key to transform the received ciphertext to plaintext.

In accordance with the present invention, for the i^{th} terminal, the encoding key E_i is a pair of positive integers e_i and n_i specifically associated with that terminal, and the decoding key is a pair of positive integers d_i and n_i where d_i is also specifically associated with that terminal. In accordance with the invention, n_i is a composite number equal to the product of prime factors p_i and q_i , e_i is relatively prime to $(p_i-1)(q_i-1)$, and d_i is a multiplicative inverse of $e_i \pmod{(p_i-1)(q_i-1)}$. By way of example, d_i can be a multiplicative inverse of $e_i \pmod{(p_i-1)(q_i-1)}$.

The encoding transformation performed by the i^{th} terminal encoding device for a message destined for the j^{th} terminal is in accordance with the relation:

$$C_j = M_i^{e_j} \pmod{n_j}.$$

The message M_i is a number in the range $0 \leq M_i \leq n_j - 1$. This condition may be met by initially transforming, or pre-coding, the message-to-be-transmitted into blocks which are in that range at the i^{th} terminal, and then recombining the blocks at the j^{th} terminal. The decoding transformation performed by the j^{th} terminal decoding device for the ciphertext received from the i^{th} terminal is in accordance with the relation:

$$M_i' = C_j^{d_j} \pmod{n_j}.$$

Accordingly, the encoding device 12 and decoding device 14 perform substantially the same functional operation but with different message inputs (M or C) and different keys (E or D). In the present exemplary embodiment which transfers an encrypted message from terminal A to terminal B, $i=A$ and $j=B$.

The FIG. 2 embodiment is also suitable for sending signed messages M_{A_s} (in lieu of C_A) from terminal A to terminal B. In this form, the system of FIG. 2 is substantially the same as that described above except that terminal A utilizes its own decoding key D_A as the "encoding key" for device 12, and terminal B utilizes terminal A's encoding key for the "decoding key" for device 14. With this configuration, M_A is in the range $0 \leq M_A \leq n_A - 1$ and terminal A transforms the message M_A to M_{A_s} in accordance with:

$$M_{A_s} = M_A^{d_A} \pmod{n_A}.$$

and terminal B transforms the received signed message M_A back to M_A in accordance with:

$$M_A = M_{A'}^{e/n} \pmod{n}$$

An exemplary form for the encoding device 12 is shown in FIG. 3. The device 12 includes an M register 20 for receiving an applied digital message-to-be-transferred and e register 22 and n register 24 for receiving an applied encoding key consisting of binary signals representative of the numbers e and n for the intended receiver terminal (which, in a public key cryptographic system, are readily available from a public file for all terminals). Encoding device 12 further includes an e shift register 26, a multiplier selector 28, ciphertext register 30 and a modulo n multiplier 32. These blocks in the device 12 are conventionally arranged together with timing control circuitry to perform "exponentiation by repeated squaring and multiplication." In alternative embodiments, other exponentiation procedures may readily be utilized in keeping with the present invention.

In the operation of device 12 after a message M is loaded into the message register 20, the ciphertext register 30 is preset to the number 1 and the e and n registers are loaded with binary words representative of the numbers e and n, respectively, for the intended receiver terminal. The shift register 26 is clocked to shift the bits of the e word so that one bit at a time starting with the most significant bit is applied to the control input of the multiplier selector 28. In response to each applied e word bit, the current contents of C register 30 are applied as a first input to multiplier 32. In addition, the selector 28 selects the contents of C register 30 as a second input to multiplier 32, and the multiplier 32 then is activated to provide an intermediate product (modulo n) of the signals at its first and second inputs, thereby effecting a squaring (modulo n) of the contents of C register 30. C register 30 is then updated with the intermediate product signal, which is in turn applied to the first input of multiplier 32. The selector 28 then selects either the contents of M register 20 (if the currently applied e word bit is 1) or binary 1 (if the currently applied e word bit is 0) as the second input of multiplier 32, and the multiplier 32 is activated to provide a final product (modulo n) of the signals at its first and second inputs. The C register 30 is then updated with the final product signal. The e shift register is then activated to shift the e word by one bit so that the next e word bit is applied to selector 28 and the above operation repeats. Following the completion of the above operation for the last bit of the e word, the contents of the C register 30 are representative of the ciphertext corresponding to the applied message M, and is ready for transmission over the communications channel 10. In alternative configurations, the transformation of the message M to the ciphertext C may be accomplished using a programmed digital computer rather than the hardware elements illustrated in FIG. 3.

The decoding device 14 is substantially the same as the illustrated encoding device illustrated in FIG. 3, except that the message applied to the register corresponding to register 20 is replaced by the ciphertext word received from the communication channel 10, and the encoding key (e, n) words applied to the registers corresponding to registers 22 and 24 are replaced by the decoding key (d, n) words for the terminal. In this configuration, the register corresponding to register 30 contains intermediate and final product signals corre-

sponding to the deciphered message M' , and the blocks corresponding to blocks 26, 28 and 32 perform the same functions in their corresponding elements in the encoding device 12, but for the numbers d and n. As in the encoding device 12, timing control circuitry is adapted to control the sequential operation of those elements in the manner described. The device of FIG. 3 is also suitable for the signed message mode of operation, with the substitution of the appropriate encoding and decoding keys.

The communications system illustrated in FIG. 2 is suitable for one-directional communicating messages from terminal A to terminal B. FIG. 4 illustrates a similar configuration which accommodates the two-way transmission of messages between terminals A and B. In a similar manner, additional terminals may be added to the network (with suitable selection of encoding keys for each desired communication) and coupled to the communications channel 10 by way of conventional modulator and demodulator networks and terminal addressing networks to control the appropriate flow of messages from originating terminal to a desired receiving terminal.

In the FIG. 4 configuration, separate encoding and decoding devices are shown for each terminal. However, as noted above, the encoding and decoding devices perform substantially the same functions but with different input message and key signals. Accordingly, each of the stations at remote locations A and B in the FIG. 4 configuration may be replaced by a single device which may be operated as either an encoding or a decoding device with appropriate switches to control the message input (M or C) and key input (E or D). In the configuration of FIG. 4, the origin for the message, reconstituted plaintext and ciphertext is denoted by subscripts representative of the respective originating terminal. In addition, the encoding and decoding keys are representative by the letters E and D with subscripts representative of the associated terminal. For example, since terminal A is communicating with terminal B, the encoding key is denoted E_B so that the decoding terminal B may apply its decoding key D_B to extract the message M' of $A (=M_A)$. For cases where terminal A wishes to communicate with a third terminal, for example, terminal C, the encoding key for the terminal A encoding device 14A would be replaced with a corresponding encoding key E_C for terminal C.

FIG. 5 shows an embodiment of a communication system in accordance with the present invention for transmitting signed messages from terminal A to terminal B over the communication channel 10. In this configuration, the terminal A includes an encoding device 12A which corresponds to the encoding device 12 in the FIG. 2 configuration and which similarly transforms a message to ciphertext using the encoding key for the intended receiver terminal (i.e., terminal B in this case). In addition, terminal A includes a decoding device 40A which is similar in form to the decoding device 14 (FIG. 2), but which utilizes the decoding key D_A associated with terminal A as the key for that device 40A. The device 40 transforms the message to be transmitted M_A to a signed message $M_{A'}$, which in turn is applied as the message word input to device 12A. Device 12A provides a signed ciphertext word $C_{A'}$ which is representative of the signed message word as enciphered for reception by terminal B. $C_{A'}$ is transferred to terminal B over channel 10.

Terminal B includes a decoding device 14B which corresponds to the decoding device 14 in the FIG. 2 configuration and which transforms received signed ciphertext word $C_{A'}$ to the signed message word $M_{A'}$ using terminal B's decoding key D_B . In addition, terminal B includes an encoding device 42B which is similar in form to the encoding device 12A, but which utilizes the signed message word $M_{A'}$ as its data input and the encoding key E_A associated with terminal A as the key for that device 42B. Device 42B transforms the signed message word $M_{A'}$ to the unsigned message word M_A , which corresponds to the original message M_A . Thus, all of the devices 12A, 14B, 40A, and 42B are substantially the same in function but they utilize the indicated encoding or decoding keys and data inputs.

In alternative embodiments, the order of the enciphering and signing operations may be switched, provided that the order of the corresponding deciphering and unsigning operations are similarly switched. Furthermore, additional levels of enciphering or signing may also be utilized so long as there is a corresponding deciphering or unsigning operation.

While the system in FIG. 5 is suitable for signal direction transmission of a message from terminal A to terminal B, terminal B may also include blocks corresponding to blocks 12A and 40A and terminal A may include blocks corresponding to blocks 14B and 42B with the respective keys E_A , D_B , D_A and E_B , as shown in FIG. 6. With the latter system, two-way signed digital communications may be accomplished. In alternative configurations, additional terminals may be utilized using the addition of similar blocks coupled to the channel 10, with the appropriate keys and modem and addressing networks.

The signature systems described above in conjunction with FIGS. 2, 4, 5, and 6 are suitable where the respective message and ciphertext words represent numbers less than the n_i for the particular transformations. As noted above, when the words to be transformed (either by encoding or decoding) are initially beyond the nominal range requirement, a blocking subsystem is used to break the word into blocks within that range before the transformation is performed. A corresponding unblocking subsystem is utilized following the inverse transformation at the receiving terminal to obtain the original message. FIG. 7 shows an exemplary configuration which is similar to the configuration of FIG. 5, but which also includes blocking and unblocking subsystems. Terminal A of the configuration of FIG. 7 includes a first blocking subsystem 61 which precodes the message to a blocked message M_A , which in turn is transformed by device 40A to a signed message $M_{A'}$. A second blocking subsystem 63 transforms $M_{A'}$ to blocks $M_{A'}$, each block of which is then transformed by device 12A to a signed ciphertext word $C_{A'}$. At terminal B, $C_{A'}$ is first transformed to signed message blocks $M_{A'}$ by device 14B, which are then transformed by a first unblocking subsystem 65 to the signed message word $M_{A'}$. The word $M_{A'}$ is then transformed by device 42B to the blocked message M_A , which is in turn transformed by a second unblocking subsystem 67 to the original message. In embodiments where the message is enciphered before signing, the device that first provides $C_{A'}$ which is transformed to $C_{A'}$ and then to C_A . At the receiving terminal C_A is first transformed to $C_{A'}$ which is then transformed to C_A and then decoded to M_A .

The blocking and unblocking subsystems may be configured with any of the various forms of the present invention wherein the respective message and ciphertext words are outside the nominal ranges. Where the range requirements for a word transformation are met, the blocking and unblocking subsystems are not utilized.

The encoding operation for the present invention will now be illustrated for the case where $p=47$, $q=59$, $n=pq=47 \cdot 59=2773$, $d=157$ and $e=17$, to encode the message:

ITS ALL GREEK TO ME

Initially, the message is encoded with two English letters in a block, by substituting for each letter a two-digit number: blank=00, A=01, B=02, ..., Z=26. In this form, the message is precoded to:

$M = 0920190001121200071805051100201500130500$

Since this value for M is greater than $n(=2773)$, M is broken into blocks M_1, \dots, M_{10} as follows:

$M = M_1 M_2 M_3 M_4 M_5 M_6 M_7 M_8 M_9 M_{10}$
 $= 0920190001121200071805051100201500130500$

Since $e=10001$ in binary, the first block ($M_1=0920$) is enciphered using the encoding key $E=(17,2773)$ to a corresponding ciphertext block C_1 :

$$\begin{aligned} C_1 &= M_1^e \pmod{n} \\ &= M_1^{17} \pmod{2773} \\ &= (((((1)^2 \cdot M_1)^2)^2)^2) \cdot M_1 \pmod{2773} \\ &= 948 \pmod{2773} \end{aligned}$$

The whole message is enciphered as:

$C = C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8 C_9 C_{10}$
 $= 0948234210841444266323900778077402191655$

The ciphertext can be deciphered in a similar manner using the decoding key $D=(157,2773)$. For the first block C_1 :

$$\begin{aligned} M_1' &= C_1^d \pmod{n} \\ &= 948^{157} \pmod{2773} \\ &= 920 \pmod{2773} \end{aligned}$$

The other blocks are similarly deciphered so that the various blocks may be put together to form M , and then be decoded (by reversing the letter-to-two-digit-number transformation) to the original message.

In a public key cryptosystem utilizing the present invention, each user has an associated encryption key $E=(e,n)$ and decryption key $D=(d,n)$, wherein the encryption keys for all users are available in a public file, while the decryption keys for the users are only known to the respective users.

In order to maintain a high level of security in such systems, a user's decoding key is not determinable in a practical manner from that user's encoding key. Since

13

$$e \cdot d \equiv 1 \pmod{1 \text{ cm}((p-1), (q-1))}$$

d can be determined from e provided p and q are also known. Accordingly, the security of the system is dependent upon the ability to determine p and q which are the prime factors of n. By selecting p and q to be large primes, the resultant composite number n is also large, and correspondingly difficult to factor. For example, using known computer-implemented factorization methods, on the order of 10^9 years is required to factor a 200 digit long number. Thus, as a practical matter, although a user's encryption key $E=(e,n)$ is public, the prime factors p and q of n are effectively hidden from anyone due to the enormous difficulty in factoring n. These aspects of the present invention are described more fully in the present inventors' publication "On Digital Signatures and Public-Key Cryptosystems", MIT/LCS/TM-82, NTIS No. ADA-039036, April 1977.

In general, the present invention provides secure communications as a practical matter because the operation of evaluating a polynomial modulo n, where n is a large composite number, may be easily inverted only with the knowledge of the factors of n. In the preferred embodiment described above, $n=p \cdot q$, where p and q are prime, and the message M is transformed by evaluating the polynomial $f(M)=M^e$ modulo n, where $\gcd(e, (p-1)(q-1))=1$.

In alternative embodiments, the present invention may use a modulus n which is a product of three or more primes (not necessarily distinct). Decoding may be performed modulo each of the prime factors of n and the results combined using "Chinese remaindering" or any equivalent method to obtain the result modulo n.

In still other embodiments, the message M may be encoded to ciphertext C by evaluating a polynomial $a_e M^e + a_{e-1} M^{e-1} + \dots + a_0$ modulo n where e and a_e, a_{e-1}, \dots, a_0 are numbers. In such embodiments, C may be decoded utilizing conventional root-finding techniques, choosing which of any roots is the proper decoded version, for example, by the internal redundancy of the message. Where e is relatively prime to the Euler totient function of n, $\phi(n)$, and where $a_e=1$ and a_{e-1}, \dots, a_0 equal zero, C may be decoded to M' in accordance with

$$M' = C^d \pmod{n}$$

where d is the multiplicative inverse of $e \pmod{\lambda(n)}$ where $\lambda(n)$ is the least positive integer such that

$$S^{\lambda(n)} \equiv 1 \pmod{n}$$

for all integers S relatively prime to n.

In yet other embodiments, the message M may be encoded to ciphertext C by the performance of an ordered succession of invertible operations (modulo n) on M, with the succession including at least exponentiation, and in various embodiments, such other invertible operations as adding, subtracting, multiplying or dividing by constants (positive or negative), and simple bit manipulations (e.g. complementing or permuting bits). Decoding is accomplished by applying a second succession of invertible operations on C, with each of the operations of the second succession corresponding to one of the operations in the encoding succession, where the operations of the second succession are in reverse order with respect to the corresponding inverse opera-

14

tions of the encoding succession. By way of example, M may be encoded to C as follows:

$$C = E(M) = (M^{13} + 2)^{17} \pmod{11 \cdot 7}$$

This ciphertext word C is decoded as

$$M = D(C) = ((C/4)^{13} - 2)^{17} \pmod{11 \cdot 7}$$

where 23 and 13 are the multiplicative inverses of 17, and 13, respectively, modulo $1 \text{ cm}(11-1, 7-1)$.

Similarly, the following variations on the use of the encoding/decoding devices are to be considered as obvious to one skilled in the prior art and therefore within the intended scope of the attached claims:

- (1) using the encoding/decoding devices in cipher-feedback mode instead of the simple block encoding method described here, or as a pseudo-random number generator for use to generate pads,
- (2) signatures may be effected by signing a transformed version of the message, where the transformation is publicly known and is not necessarily invertible. (It may, for example, compress the message to be signed into a shorter form, thus giving shorter signatures).
- (3) using the present invention to transmit keys to be used in another encryption method for encoding subsequent messages.

The invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The present embodiments are therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than by the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

We claim:

1. A cryptographic communications system comprising:
 - A. a communications channel,
 - B. an encoding means coupled to said channel and adapted for transforming a transmit message word signal M to a ciphertext word signal C and for transmitting C on said channel, where M corresponds to a number representative of a message and

$$0 \leq M \leq n-1$$

where n is a composite number of the form

$$n = p \cdot q$$

where p and q are prime numbers, and where C corresponds to a number representative of an enciphered form of said message and corresponds to

$$C = M^e \pmod{n}$$

where e is a number relatively prime to $1 \text{ cm}(p-1, q-1)$, and

- C. a decoding means coupled to said channel and adapted for receiving C from said channel and for transforming C to a receive message word signal M'

where M' corresponds to a number representative of a deciphered form of C and corresponds to

$$M' = C^d \pmod{n}$$

where d is a multiplicative inverse of $e \pmod{1 \text{ cm}((p-1), (q-1))}$.

2. A system according to claim 1 wherein at least one of said transforming means comprises:
 - a first register means for receiving and storing a first digital signal representative of said signal-to-be-transformed,
 - a second register means for receiving and storing a second digital signal representative of the exponent of the equivalence relation defining said transformation,
 - a third register means for receiving and storing a third digital signal representative of the modulus of the equivalency relation defining said transformation, and
 - an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:
 - A. an output register means for receiving and storing a first multiplier signal and for applying said first multiplier signal to a first multiplier input line,
 - B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,
 - C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and
 - D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.
3. A communications system for transferring message signals M_i comprising k terminals, wherein each terminal is characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$, where $i=1, 2, \dots, k$, and wherein

M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal, and

$$0 \leq M_i \leq n_i - 1,$$

n_i is a composite number of the form

$$n_i = p_i q_i$$

p_i and q_i are prime numbers,
 e_i is relatively prime to $1 \text{ cm}((p_i-1), (q_i-1))$,
 d_i is a multiplicative inverse of

$$e_i \pmod{1 \text{ cm}((p_i-1), (q_i-1))}$$

wherein a first terminal includes means for encoding a digital message word signal M_A for transmission from said first terminal ($i=A$) to a second terminal ($i=B$), said first terminal including:

means for transforming said message word signal M_A to a signed message word signal M_{A_s} , M_{A_s} corresponding to a number representative of an encoded form of said message word signal M_A , whereby:

$$M_{A_s} = M_A^{e_A} \pmod{n_A}.$$

4. A system according to claim 3 wherein at least one of said transforming means comprises:

- a first register means for receiving and storing a first digital signal representative of said signal-to-be-transformed,
- a second register means for receiving and storing a second digital signal representative of the exponent of the equivalence relation defining said transformation,
- a third register means for receiving and storing a third digital signal representative of the modulus of the equivalency relation defining said transformation, and
- an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:
 - A. an output register means for receiving and storing a first multiplier signal and for applying said first multiplier signal to a first multiplier input line,
 - B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,
 - C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and
 - D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

5. The system of claim 3 further comprising: means for transmitting said signal message word signal M_{A_s} from said first terminal to said second terminal, and

wherein said second terminal includes means for decoding said signed message word signal M_{A_s} to said message word signal M_A , said second terminal including:

means for transforming said ciphertext word signal C_A to said message word signal M_A , whereby

$$M_A = M_{A_s}^{d_A} \pmod{n_A}.$$

6. The system of claim 3 wherein said encoding means further comprises:

17

means for transforming said signed message word signal M_A to one or more signed message block word signals M_{A_i} , each block word signal M_{A_i} corresponding to a number representative of a portion of said signed message word signal M_A in the range $0 \leq M_{A_i} \leq n_B - 1$, and
 means for transforming each of said signed message block word signals M_{A_i} to a signed ciphertext word signal C_{A_i} , C_{A_i} corresponding to a number representative of an encoded form of said signed message block word signal, whereby

$$C_{A_i} = M_{A_i}^{e_i} \pmod{n_B}$$

7. The system of claim 6 comprising the further steps of:

means for transmitting said signed ciphertext word signal C_{A_i} from said first terminal to said second terminal,
 wherein said second terminal includes means for decoding said signed ciphertext word signals to said message word signal M_A , said second terminal including:
 means for transforming each of said signed ciphertext word signals C_{A_i} to one of said signed message block word signals M_{A_i} , whereby

$$M_{A_i} = C_{A_i}^{d_i} \pmod{n_B}$$

means for transforming said signed message block word signals to said signed message word signal M_A

means for transforming said signed message word signal to said message word signal M_A , whereby

$$M_A = M_{A_i}^{e_i} \pmod{n_A}$$

8. A communications system for transferring a message signal M_i comprising k terminals, wherein each terminal is characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$, where $i = 1, 2, \dots, k$, and wherein

M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal, n_i is a composite number of the form

$$n_i = p_i q_i$$

p_i and q_i are prime numbers,
 e_i is relatively prime to $1 \pmod{(p_i - 1)(q_i - 1)}$,
 d_i is a multiplicative inverse of

$$e_i \pmod{(1 \pmod{(p_i - 1)(q_i - 1)})}$$

wherein a first terminal includes means for encoding a digital message word signal M_A for transmission from said first terminal ($i = A$) to a second terminal ($i = B$), said first terminal including:

means for transforming said message word signal M_A to one or more message block word signals M_{A_i} , each block word signal M_{A_i} being a number representative of a portion of said message word signal M_A in the range $0 \leq M_{A_i} \leq n_B - 1$, means for transforming each of said message block word signals M_{A_i} to a ciphertext word signal C_{A_i} , C_{A_i} corresponding to a number representative of an encoded form of said message block word signal M_{A_i} , whereby:

$$C_{A_i} = M_{A_i}^{e_i} \pmod{n_B}$$

18

9. A system according to claim 8 wherein at least one of said transforming means comprises:

a first register means for receiving and storing a first digital signal representative of said signal-to-be-transformed,
 a second register means for receiving and storing a second digital signal representative of the exponent of the equivalence relation defining said transformation,
 a third register means for receiving and storing a third digital signal representative of the modulus of the equivalency relation defining said transformation, and

an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:

A. an output register means for receiving and storing a first multiplier signal and for applying said first multiplier signal to a first multiplier input line,

B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,

C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and

D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

10. The system of claim 8 further comprising:

means for transmitting said ciphertext word signals from said first terminal to said second terminal, and wherein said second terminal includes means for decoding said ciphertext word signals to said message word signal M_A , said second terminal including:

means for transforming each of said ciphertext word signals C_{A_i} to one of said message block word signals M_{A_i} , whereby

$$M_{A_i} = C_{A_i}^{d_i} \pmod{n_B}$$

means for transforming said message block word signals M_{A_i} to said message word signal M_A .

11. The system of claim 8 wherein said encoding means further comprises:

means for transforming said ciphertext word signal C_A to one or more ciphertext block word signals C_{A_i} , each block word signal C_{A_i} being a number representative of a portion of said ciphertext word signal C_A in the range $0 \leq C_{A_i} \leq n_A - 1$,

means for transforming each of said ciphertext block word signals C_{A_i} to a signed ciphertext word signal C_{A_i} corresponding to a number representative

19

of an encoded form of said ciphertext block word signal C_A' , whereby

$$C_A' = C_A^{e_A} \pmod{n_A}$$

12. The system of claim 11 further comprising:
means for transmitting said signed ciphertext word signals from said first terminal to said second terminal,

wherein said second terminal includes means for decoding said signed ciphertext word signals to said message word signal M_A , said second terminal including:
means for transforming each of said signed ciphertext word signals C_A' to one of said ciphertext block word signals C_A , whereby

$$C_A = C_A'^{d_A} \pmod{n_A}$$

means for transforming said ciphertext block word signals to said message block word signals, whereby

$$M_A' = C_A^{d_B} \pmod{n_B}$$

means for transforming said message block word signals to said message word signal M_A .

13. A communications system having a plurality of terminals coupled by a communications channel, including a first terminal characterized by an associated encoding key $E_A = (e_A, n_A)$ and decoding key $D_A = (d_A, n_A)$, and including a second terminal, wherein n_A is a composite number of the form

$$n_A = p_A q_A$$

p_A and q_A are prime numbers,
 e_A is relatively prime to $1 \text{ cm}(p_A - 1, q_A - 1)$,
 d_A is a multiplicative inverse of
 $e_A \pmod{1 \text{ cm}((p_A - 1), (q_A - 1))}$,

wherein said first terminal comprises:

encoding means coupled to said channel and adapted for transforming a transmit message word signal M_A to a signed message word signal M_A' and for transmitting M_A' on said channel,
where M_A corresponds to a number representative of a message and

$$0 \leq M_A \leq n_A - 1$$

where M_A' corresponds to a number representative of a signed form of said message and corresponds to

$$M_A' = M_A^{e_A} \pmod{n_A}$$

wherein said second terminal comprises:

decoding means coupled to said channel and adapted for receiving M_A' from said channel and for transforming M_A' to a receive message word signal M_A where M_A' corresponds to a number representative of an unsigned form of M_A and corresponds to

$$M_A' = M_A^{e_A} \pmod{n_A}$$

14. A system according to claim 13 wherein at least one of said transforming means comprises:

a first register means for receiving and storing a first digital signal representative of said signal-to-be-transformed,
a second register means for receiving and storing a second digital signal representative of the exponent

20

of the equivalence relation defining said transformation,

a third register means for receiving and storing a third digital signal representative of the modulus of the equivalence relation defining said transformation, and

an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:

A. an output register means for receiving and storing a first multiplier signal and for applying said first multiplier signal to a first multiplier input line,

B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,

C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and

D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

15. The system according to claim 13 wherein said second terminal is characterized by an associated encoding key $E_B = (e_B, n_B)$ and decoding key $D_B = (d_B, n_B)$, where:

n_B is a composite number of the form

$$n_B = p_B q_B$$

p_B and q_B are prime numbers,
 e_B is relatively prime to $1 \text{ cm}(p_B - 1, q_B - 1)$,
 d_B is a multiplicative inverse of

$$e_B \pmod{1 \text{ cm}((p_B - 1), (q_B - 1))}$$

wherein said second terminal comprises:

encoding means coupled to said channel and adapted for transforming a transmit message word signal M_B to a signed message word signal M_B' and for transmitting M_B' on said channel,

where M_B corresponds to a number representative of a message and

$$0 \leq M_B \leq n_B - 1$$

where M_B' corresponds to a number representative of an enciphered form of said message signal M_B and corresponds to

$$M_B' = M_B^{e_B} \pmod{n_B}$$

wherein said first terminal comprises:

21

decoding means coupled to said channel and adapted for receiving $M_{B'}$ from said channel and for transforming $M_{B'}$ to a receive message word signal M_B' where M' is a number representative of an unsigned form of C and corresponds to

$$M_B' = M_{B'}^{e_B} \pmod{n_B}$$

16. The system according to claim 13 wherein said second terminal is characterized by an associated encoding key $E_B = (e_B, n_B)$ and decoding key $D_B = (d_B, n_B)$, where:

n_B is a composite number of the form:

$$n_B = p_B q_B$$

p_B and q_B are prime numbers,
 e_B is relatively prime to $1 \text{ cm}(p_B - 1, q_B - 1)$,
 d_B is a multiplicative inverse of $e_B \pmod{1 \text{ cm}((p_B - 1), (q_B - 1))}$,

wherein said encoding means of said first terminal is adapted for transforming said message word signal M_A to a signed ciphertext word signal $C_{A'}$ and for transmitting $C_{A'}$ on said channel in place of $M_{A'}$ whereby $C_{A'}$ corresponds to a number representative of a signed enciphered form of said message and corresponds to:

$$C_{A'} = M_{A'}^{e_A} \pmod{n_A}$$

where $M_{A'}$ corresponds to a number representative of a block of said signed message word signal $M_{A'}$ in the range $0 \leq M_{A'} \leq n_A - 1$ wherein said decoding means of said second terminal is adapted to first transform said signed enciphered form of said message $C_{A'}$ to $M_{A'}$ in accordance with:

$$M_{A'} = C_{A'}^{d_A} \pmod{n_A}$$

then to transform $M_{A'}$ to $M_{A''}$ and then to transform $M_{A''}$ to said receive message word signal M_A' , where M_A' is a number representative of a deciphered form of $C_{A'}$ and corresponds to

$$M_{A'} = M_{A'}^{e_A} \pmod{n_A}$$

17. The system according to claim 15 wherein said encoding means of said first terminal is adapted for transforming said message word signal M_A to a signed ciphertext word signal $C_{A'}$ and for transmitting $C_{A'}$ on said channel in place of $M_{A'}$ whereby $C_{A'}$ corresponds to a number representative of a signed enciphered form of said message and corresponds to:

$$C_{A'} = M_{A'}^{e_A} \pmod{n_A}$$

wherein said decoding means of said second terminal is adapted to first transform said signed enciphered form of said message $C_{A'}$ to $M_{A'}$ in accordance with:

$$M_{A'} = C_{A'}^{d_A} \pmod{n_A}$$

then to transform $M_{A'}$ to $M_{A''}$ and then to transform $M_{A''}$ to said receive message word signal M_A' , where M_A' corresponds to a number representative of a deciphered form of $C_{A'}$ and corresponds to

$$M_{A'} = M_{A'}^{e_A} \pmod{n_A}$$

22

wherein further said encoding means of said second terminal is adapted for transforming said message word signal M_B to a signed ciphertext word signal $C_{B'}$ and for transmitting $C_{B'}$ on said channel in place of $M_{B'}$,

whereby $C_{B'}$ corresponds to a number representative of a signed enciphered form of said message and corresponds to:

$$C_{B'} = M_{B'}^{e_B} \pmod{n_B}$$

where $M_{B'}$ corresponds to a number representative of a block of said signed message word signal $M_{B'}$ in the range $0 \leq M_{B'} \leq n_B - 1$, wherein said decoding means of said first terminal is adapted to first transform said signed enciphered form of said message $C_{B'}$ to $M_{B'}$ in accordance with:

$$M_{B'} = C_{B'}^{d_B} \pmod{n_B}$$

then to transform $M_{B'}$ to M_B , and then to transform M_B to said receive message word signal M_B' , and corresponds to

$$M_B' = M_{B'}^{e_B} \pmod{n_B}$$

18. A cryptographic communications system having a plurality of terminals coupled by a communications channel, including a first terminal characterized by an associated encoding key $E_A = (e_A, n_A)$ and decoding key $D_A = (d_A, n_A)$, and including a second terminal wherein n_A is a composite number of the form

$$n_A = p_A q_A$$

p_A and q_A are prime numbers,
 e_A is relatively prime to $1 \text{ cm}(p_A - 1, q_A - 1)$,
 d_A is a multiplicative inverse of

$$e_A \pmod{1 \text{ cm}((p_A - 1), (q_A - 1))}$$

wherein said second terminal comprises:

blocking means for transforming a message-to-be-transmitted from said second terminal to said first terminal, to one or more transmit message word signals M_B ,

where M_B corresponds to a number representative of said message in the range

$$0 \leq M_B \leq n_A - 1$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_B to a ciphertext word signal C_B and for transmitting C_B on said channel, where C_B corresponds to a number representative of an enciphered form of said message and corresponds to

$$C_B = M_B^{e_A} \pmod{n_A}$$

wherein said first terminal comprises:

decoding means coupled to said channel and adapted for receiving said ciphertext word signals C_B from said channel and for transforming each of said ciphertext word signals to a receive message word signal M_B , and

means for transforming said receive message word signals M_B to said message.

where M_B' is a number representative of a deciphered form of C_B and corresponds to

$$M_B' = C_B^{d_A} \pmod{n_A}$$

19. A system according to claim 18 wherein at least one of said transforming means comprises:

a first register means for receiving and storing a first digital signal representative of said signal-to-be-transformed,
a second register means for receiving and storing a second digital signal representative of the exponent of the equivalence relation defining said transformation,

a third register means for receiving and storing a third digital signal representative of the modulus of the equivalency relation defining said transformation, and

an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:

A. an output register means for receiving and storing a first multiplier signal and for applying said first multiplier signal to a first multiplier input line,

B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,

C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and

D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

20. The system according to claim 18 wherein said second terminal is characterized by an associated encoding key $E_B = (e_B, n_B)$ and decoding key $D_B = (d_B, n_B)$, where:

n_B is a composite number of the form

$$n_B = p_B q_B$$

p_B and q_B are prime numbers,
 e_B is relatively prime to $1 \text{ cm}(p_B - 1, q_B - 1)$,
 d_B is a multiplicative inverse of

$$e_B \pmod{1 \text{ cm}((p_B - 1)(q_B - 1))}$$

wherein said first terminal comprises:

blocking means for transforming a message-to-be-transmitted from said first terminal to said second terminal, to one or more transmit message word signals M_A ,

where M_A corresponds to a number representative of said message in the range

$$0 \leq M_A \leq n_B - 1$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_A to a ciphertext word signal C_A and for transmitting C_A on said channel,

where C_A corresponds to a number representative of an enciphered form of said message and corresponds to

$$C_A = M_A^{e_B} \pmod{n_B}$$

wherein said second terminal comprises:

decoding means coupled to said channel and adapted for receiving said ciphertext word signals C_A from said channel and for transforming each of said ciphertext word signals to a receive message word signal M_A' , and

means for transforming said receive message word signals M_A' to said message,

where M' corresponds to a number representative of a deciphered form of C and corresponds to

$$M_A' = C_A^{d_B} \pmod{n_B}$$

21. The system according to claim 18 wherein said second terminal is characterized by an associated encoding key $E_B = (e_B, n_B)$ and decoding key $D_B = (d_B, n_B)$, where:

n_B is a composite number of the form

$$n_B = p_B q_B$$

p_B and q_B are prime numbers,
 e_B is relatively prime to $1 \text{ cm}(p_B - 1, q_B - 1)$,
 d_B is a multiplicative inverse of

$$e_B \pmod{1 \text{ cm}((p_B - 1)(q_B - 1))}$$

wherein said encoding means of said second terminal is adapted for transforming said message word signal M_B to a signed cipher-text word signal $C_{B'}$ and for transmitting $C_{B'}$ on said channel in place of C_B , whereby $C_{B'}$ corresponds to a number representative of a signed enciphered form of said message and corresponds to:

$$C_{B'} = C_B^{e_B} \pmod{n_B}$$

where C_B'' corresponds to a number representative of a block of said ciphertext word signal C_B in the range $0 \leq C_B'' \leq n_B - 1$,

wherein said decoding means of said first terminal is adapted to first transform said signed enciphered form of said message $C_{B'}$ to C_B'' in accordance with:

$$C_B'' = C_{B'}^{d_B} \pmod{n_B}$$

then to transform C_B'' to C_B , and then to transform C_B to said receive message word signal M_B' , where M_B' corresponds to a number representative of a deciphered form of $C_{B'}$ and corresponds to:

$$M_B' = C_B^{d_A} \pmod{n_A}$$

22. The system according to claim 20 wherein said encoding means of said second terminal is adapted for transforming said message word signal M_B to a signed ciphertext word signal $C_{B'}$ and for transmitting $C_{B'}$ on said channel in place of C_B , whereby $C_{B'}$ corresponds to a number representative of a signed enciphered form of said message and corresponds to:

25

$$C_B = C_B^{d_B} \pmod{n_B}$$

where C_B'' corresponds to a number representative of a block of said ciphertext word signal C_B in the range $0 \leq C_B'' \leq n_B - 1$, wherein said decoding means of said first terminal is adapted to first transform said signed enciphered form of said message C_B to C_B'' in accordance with:

$$C_B'' = C_B^{e_B} \pmod{n_B}$$

and then to transform C_B to C_B' , and then to transform C_B' to said receive message word signal M_B' , where M_B' is a number representative of a deciphered form of C_B and corresponds to:

$$M_B' = C_B^{d_B} \pmod{n_B}$$

wherein further said encoding means of said first terminal is adapted to transform said message word signal M_A to a signal ciphertext word signal C_A , as for transmitting C_A on said channel in place of C_B , whereby C_A corresponds to a number representative of a signed enciphered form of said message and corresponds to:

$$C_A = C_A^{d_A} \pmod{n_A}$$

where C_A'' corresponds to a number representative of a block of said ciphertext word signal C_A in the range of $0 \leq C_A'' \leq n_A - 1$, wherein said decoding means of said second terminal is adapted to first transform said signed enciphered form of said message C_A to C_A'' in accordance with:

$$C_A'' = C_A^{e_A} \pmod{n_A}$$

then to transform C_A'' to C_A , and then to transform C_A to said receive message word signal M_A' , where M_A' corresponds to a number representative of a deciphered form of C_A and corresponds to:

$$M_A' = C_A^{d_A} \pmod{n_A}$$

23. A method for establishing cryptographic communications comprising the step of:

encoding a digital message word signal M to a ciphertext word signal C , where M corresponds to a number representative of a message and

$$0 \leq M \leq n - 1$$

where n is a composite number of the form

$$n = p \cdot q$$

where p and q are prime numbers, and where C is a number representative of an encoded form of message word M , wherein said encoding step comprises the step of: transforming said message word signal M to said ciphertext word signal C whereby

$$C = M^e \pmod{n}$$

where e is a number relatively prime to $(p-1)(q-1)$.

26

24. The method according to claim 23 comprising the further step of:

decoding said ciphertext word signal C to said message word signal M ,

wherein said decoding step comprises the step of: transforming said ciphertext word signal C , whereby:

$$M = C^d \pmod{n}$$

where d is a multiplicative inverse of $e \pmod{1 \text{ cm}((p-1), (q-1))}$.

25. A method for transferring a message signal M_i in a communications system having k terminals, wherein each terminal is characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$, where $i = 1, 2, \dots, k$, and wherein

M_i corresponds to a number representative of message-to-be-transmitted from the i^{th} terminal, and

$$0 \leq M_i \leq n_i - 1$$

n_i is a composite number of the form

$$n_i = p_i \cdot q_i$$

p_i and q_i are prime numbers, e_i is relatively prime to $1 \text{ cm}(p_i - 1, q_i - 1)$, d_i is a multiplicative inverse of

$$e_i \pmod{1 \text{ cm}((p_i - 1), (q_i - 1))}$$

comprising the step of:

encoding a digital message word signal M_A for transmission from a first terminal ($i=A$) to a second terminal ($i=B$), said encoding step including the sub-step of:

transforming said message word signal M_A to a signed message word signal $M_{A'}$, $M_{A'}$ corresponding to a number representative of an encoded form of said message word signal M_A , whereby:

$$M_{A'} = M_A^{d_A} \pmod{n_A}$$

26. The method of claim 25 comprising the further steps of:

transmitting said signed message word signal $M_{A'}$ to said second terminal, and

decoding said signed message word signal $M_{A'}$ to said message word signal M_A , said decoding step including the sub-step of:

transforming said ciphertext word signal C_A to said message word signal M_A , whereby

$$M_A = M_{A'}^{e_A} \pmod{n_A}$$

27. The method of claim 25 wherein said encoding step comprises the further steps of:

transforming said signed message word signal $M_{A'}$ one or more signed message block word signals $M_{A''}$,

each block word signal $M_{A''}$ corresponding to a number representative of a portion of said signed message word signal $M_{A'}$ in the range $0 \leq M_{A''} \leq n_B - 1$, and

transforming each of said signed message block word signals $M_{A''}$ to a signed ciphertext word signal $C_{A''}$, $C_{A''}$ corresponding to a number representative of an encoded form of said signed message block word signal, whereby

$$C_{A''} = M_{A''}^{e_B} \pmod{n_B}$$

28. The method of claim 26 comprising the further steps of:
transmitting said signed ciphertext word signal C_{A_i} to said second terminal,
decoding said signed ciphertext words to said message word signal M_A , said decoding step including the sub-steps of:
transforming each of said signed ciphertext word signals C_{A_i} to one of said signed message block word signals M_{A_i}'' , whereby

$$M_{A_i}'' = C_{A_i}^{d_i} \pmod{n_i}$$

transforming said signed message block word signals to said signed message word signal M_{A_i} ,
transforming said signed message word signal to said message word signal M_A , whereby

$$M_A = M_{A_i}^{e_i} \pmod{n_i}$$

29. A method for transferring a message signal M_i in a communications system having k terminals, wherein each terminal is characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$, where $i = 1, 2, \dots, k$, and wherein

M_i corresponds to a number representative of a message-to-be-transmitted from the i^{th} terminal,
 n_i is a composite number of the form

$$n_i = p_i q_i$$

p_i and q_i are prime numbers,
 e_i is relatively prime to $1 \pmod{(p_i - 1, q_i - 1)}$,
 d_i is a multiplicative inverse of

$$e_i \pmod{(1 \pmod{(p_i - 1, q_i - 1)})}$$

comprising the step of:

encoding a digital message word signal M_A for transmission from a first terminal ($i=A$) to a second terminal ($i=B$), said encoding step including the sub-step of:

transforming said message word signal M_A to one or more message block word signals M_{A_i}'' , each block word signal M_{A_i}'' corresponding to a number representative of a portion of said message word signal M_A in the range $0 \leq M_{A_i}'' \leq n_i - 1$,
transforming each of said message block word signals M_{A_i}'' to a ciphertext word signal C_{A_i} , C_{A_i} corresponding to a number representative of an encoded form of said message block word signal M_{A_i}'' , whereby:

$$C_{A_i} = M_{A_i}^{e_i} \pmod{n_i}$$

30. The method of claim 29 comprising the further steps of:

transmitting said ciphertext word signals to said second terminal, and
decoding said ciphertext word signals to said message word signal M_A , said decoding step including the sub-steps of:

transforming each of said ciphertext word signals C_{A_i} to one or said message block word signals M_{A_i}'' , whereby

$$M_{A_i}'' = C_{A_i}^{d_i} \pmod{n_i}$$

transforming said message block word signals M_{A_i}'' to said message word signal M_A .

31. The method of claim 29 wherein said encoding step comprises the further step of:

transforming said ciphertext word signal C_{A_i} to one or more ciphertext block word signals C_{A_i}'' , each block word signal C_{A_i}'' corresponding to a number representative of a portion of said ciphertext word signal C_{A_i} in the range $0 \leq C_{A_i}'' \leq n_i - 1$,

transforming each of said ciphertext block word signals C_{A_i}'' to a signed ciphertext word signal C_{A_i} , C_{A_i} corresponding to a number representative of an encoded form of said ciphertext block word signal C_{A_i}'' , whereby

$$C_{A_i} = C_{A_i}^{d_i} \pmod{n_i}$$

32. The method of claim 31 comprising the further steps of:

transmitting said signed ciphertext word signals to said second terminal,
decoding said signed ciphertext word signals to said message word signal M_A , said decoding step including the sub-steps of:

transforming each of said signed ciphertext word signals C_{A_i} to one of said ciphertext block word signals C_{A_i}'' , whereby

$$C_{A_i}'' = C_{A_i}^{d_i} \pmod{n_i}$$

transforming said ciphertext block word signals to said message block word signals, whereby

$$M_{A_i}'' = C_{A_i}^{d_i} \pmod{n_i}$$

transforming said message block word signals to said message word signal M_A .

33. In a communications system,
an encoding means for transforming a transmit message word signal M to a ciphertext word signal C where M corresponds to a number representative of a message and

$$0 \leq M \leq n - 1$$

where n is a composite number, and
where C corresponds to a number representative of an enciphered form of said message and corresponds to

$$C = a_0 M^e + a_1 M^{e-1} + \dots + a_{n-1} \pmod{n}$$

where e and a_0, a_1, \dots, a_{n-1} are numbers.

34. A system according to claim 28 wherein at least one of said transforming means comprises:

a first register means for receiving and storing a first digital signal representative of said signal-to-be-transformed,

a second register means for receiving and storing a second digital signal representative of the exponent of the equivalence relation defining said transformation,

a third register means for receiving and storing a third digital signal representative of the modulus of the equivalency relation defining said transformation, and

an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:

A. an output register means for receiving and storing a first multiplier signal and for applying said

29

first multiplier signal to a first multiplier input line,

B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,

C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and

D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

35. In the communications system according to claim 33 where e is relatively prime to the Euler totient function of n , $\phi(n)$, and where $a_e = 1$ and a_{e-1}, \dots, a_0 equal zero,

a decoding means adapted for receiving C and for transforming C to a receive message word signal M' ,

where M' corresponds to a number representative of a deciphered form of C and corresponds to

$$M' = C^d \pmod{n}$$

where d is a multiplicative inverse of $e \pmod{\lambda(n)}$ where $\lambda(n)$ is the least positive integer such that

$$S^{\lambda(n)} = 1 \pmod{n}$$

for all integers S relatively prime to n .

36. In the communications system according to claim 33 where said encoding means is adapted to transform M to C by the performance of a first ordered succession of invertible operations on M , at least one of said operations being exponentiation, a decoding means adapted to transform C to M by the performance of a second ordered succession of invertible operations on C , wherein each of the invertible operations of said second succession is the inverse of a corresponding one of said first succession, and wherein the order of said operations in said second succession is reversed with respect to the order of corresponding operations in said first succession.

37. A method for establishing cryptographic communications comprising the step of:

encoding a digital message word signal M to a ciphertext word signal C , where M corresponds to a number representative of a message and

$$0 \leq M \leq n-1$$

where n is a composite number and where C corresponds to a number representative of an encoded form of message word M , wherein said encoding step comprises the step of:

30

transforming said message word signal M to said ciphertext word signal C whereby

$$C = a_e M^e + a_{e-1} M^{e-1} + \dots + a_0 \pmod{n}$$

where e and a_e, a_{e-1}, \dots, a_0 are numbers.

38. In the method according to claim 37 where e is relatively prime to the Euler totient function of n , $\phi(n)$, and where $a_e = 1$ and a_{e-1}, \dots, a_0 equal zero, the further step of:

decoding said ciphertext word signal C to said message word signal M ,

wherein said decoding step comprises the step of: transforming said ciphertext word signal C , whereby:

$$M = C^d \pmod{n}$$

where d is a multiplicative inverse of $e \pmod{\lambda(n)}$ where $\lambda(n)$ is the least positive integer such that

$$S^{\lambda(n)} = 1 \pmod{n}$$

for all integers S relatively prime to n .

39. In the method according to claim 37 where said encoding step includes the step of transforming M to C by the performance of a first ordered succession of invertible operations on M , the further step of:

decoding C to M by the performance of a second ordered succession of invertible operations on C , where each of the invertible operations of said second succession is the inverse of a corresponding one of said first succession, and wherein the order of said operations in said second succession is reversed with respect to the order of corresponding operations in said first succession.

40. A method according to claims 23 or 24 or 25 or 26 or 27 or 28 or 29 or 30 or 31 or 32 or 37 or 38 or 39 wherein at least one of said transforming means comprises the steps of:

receiving and storing a first digital signal in a first register, said first digital signal being representative of said word-to-be-transformed;

receiving and storing a second digital signal in a second register, said second digital signal being representative of the exponent of the equivalence relation defining said transformation,

receiving and storing a third digital signal in a third register, said third digital signal being representative of the modulus of the equivalency relation defining said transformation, and

exponentiating said first digital signal by repeated squaring and multiplication using said second and third digital signals, said exponentiating step including the substeps of:

A. receiving and storing a first multiplier signal in an output register, and applying said first multiplier signal to a first multiplier input line,

B. successively selecting each of the bits of said second digital signal as a multiplier selector, and

C. for each of said multiplier selectors, selecting as a second multiplier signal either the contents of said output register or the contents of said first register, and for applying said second multiplier signal to a second multiplier output line, said selection being dependent on the binary value of the successive bits of said second digital signal,

D. for each of said multiplier selectors, generating said first multiplier signal in a modulo multiplier

4,405,829

31

in response to the first and second multiplier signals on said first and second multiplier input lines, and for transferring said generated first multiplier signal to said output register, said first multiplier signal initially being representative of 5

32

binary 1 and thereafter being representative of the modulo product of said first and second multipliers, where the modulus of said modulo product corresponds to said third digital signal.

* * * *

10

15

20

25

30

35

40

45

50

55

60

65

STAM0041701

United States Patent [19]
Hellman et al.

[11] 4,200,770
[45] Apr. 29, 1980

[54] CRYPTOGRAPHIC APPARATUS AND METHOD

[75] Inventors: Martin E. Hellman, Stanford; Bailey W. Diffie, Berkeley; Ralph C. Merkle, Palo Alto, all of Calif.

[73] Assignee: Stanford University, Palo Alto, Calif.

[21] Appl. No.: 830,754

[22] Filed: Sep. 6, 1977

[51] Int. Cl.² H04L 9/04

[52] U.S. Cl. 178/22; 340/149 R;
375/2; 455/26

[58] Field of Search 178/22; 340/149 R

[56] References Cited

PUBLICATIONS

"New Directions in Cryptography", Diffie et al., *IEEE Transactions on Information Theory*, vol. IT-22, No. 6, Nov. 1976.

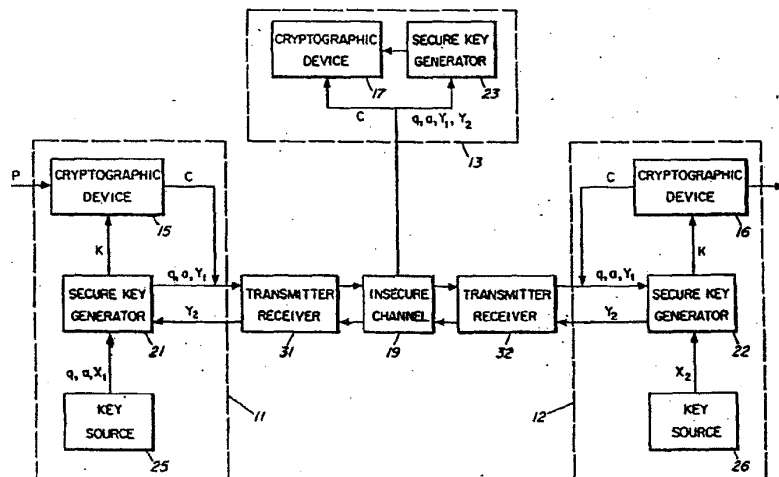
Diffie & Hellman, Multi-User Cryptographic Techniques", *AFIPS Conference Proceedings*, vol. 45, pp. 109-112, Jun. 8, 1976.

Primary Examiner—Howard A. Birmiel
Attorney, Agent, or Firm—Flehr, Hobbach, Test

[57] ABSTRACT

A cryptographic system transmits a computationally secure cryptogram over an insecure communication channel without prearrangement of a cipher key. A secure cipher key is generated by the conversers from transformations of exchanged transformed signals. The conversers each possess a secret signal and exchange an initial transformation of the secret signal with the other converser. The received transformation of the other converser's secret signal is again transformed with the receiving converser's secret signal to generate a secure cipher key. The transformations use non-secret operations that are easily performed but extremely difficult to invert. It is infeasible for an eavesdropper to invert the initial transformation to obtain either conversers' secret signal, or duplicate the latter transformation to obtain the secure cipher key.

8 Claims, 6 Drawing Figures



STAM0041702

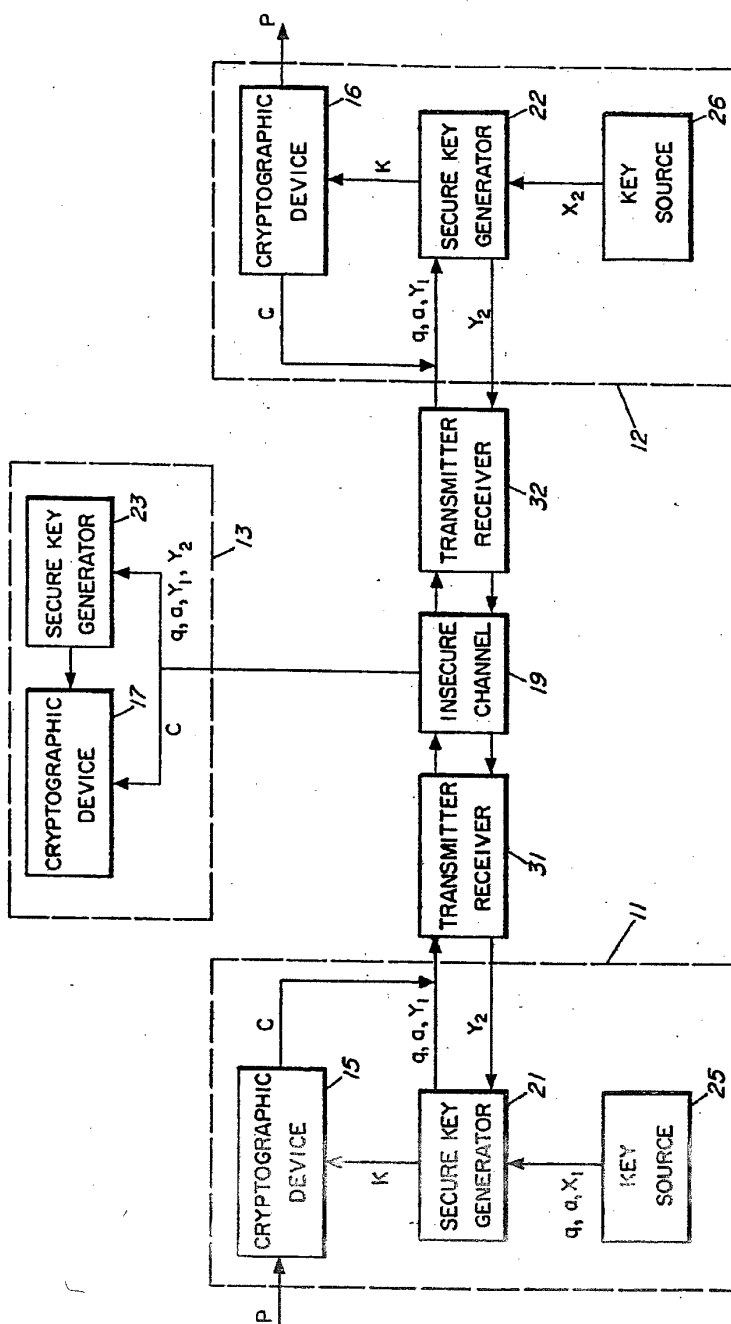


FIG. 1

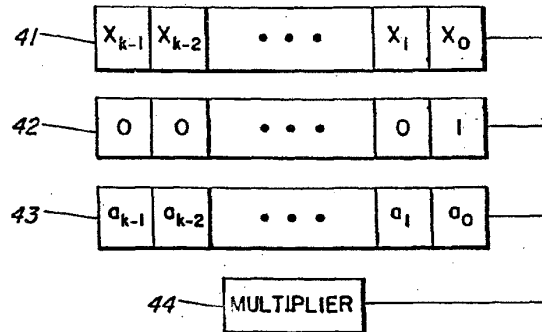


FIG. 2

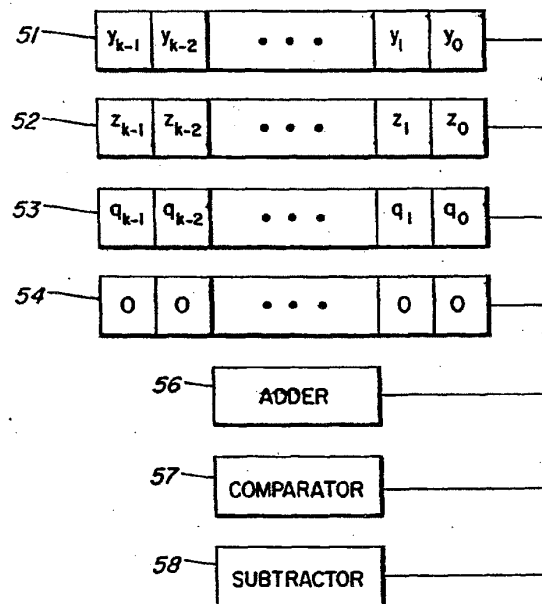


FIG. 3

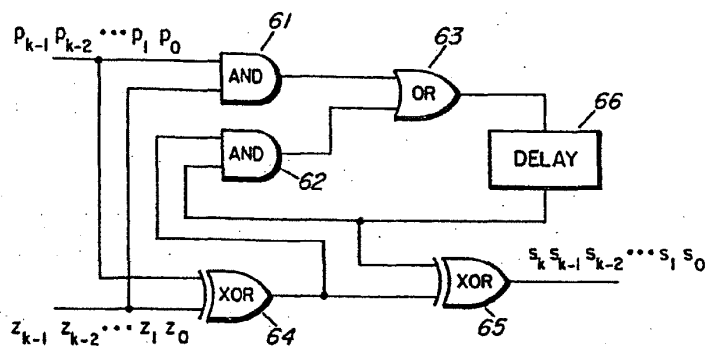


FIG. 4

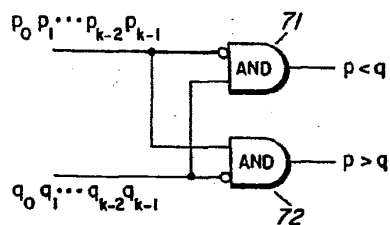


FIG. 5

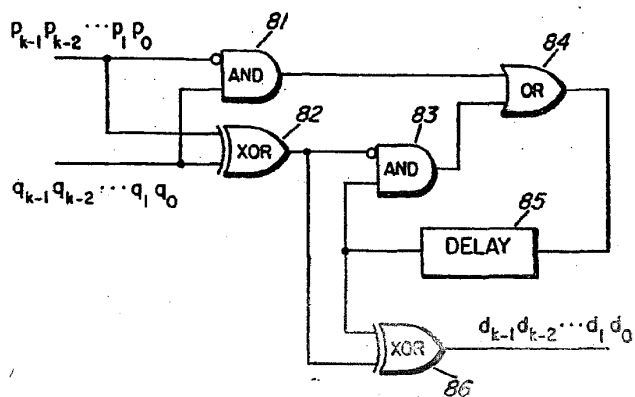


FIG. 6

CRYPTOGRAPHIC APPARATUS AND METHOD

The Government has rights in this invention pursuant to Grant No. ENG-10173 of the National Science Foundation and IPA No. 0005.

BACKGROUND OF THE INVENTION

1. Field of Invention

The invention relates to cryptographic systems.

2. Description of Prior Art

Cryptographic systems are widely used to ensure the privacy and authenticity of messages communicated over insecure channels. A privacy system prevents the extraction of information by unauthorized parties from messages transmitted over an insecure channel, thus assuring the sender of a message that it is being read only by the intended receiver. An authentication system prevents the unauthorized injection of messages into an insecure channel, assuring the receiver of the message of the legitimacy of its sender.

One of the principal difficulties with existing cryptographic systems is the need for the sender and receiver to exchange a cipher key over a secure channel to which the unauthorized party does not have access. The exchange of a cipher key frequently is done by sending the key in advance over a secure channel such as private courier or registered mail; such secure channels are usually slow and expensive.

Diffie, et al, in "Multiuser Cryptographic Techniques," *AFIPS—Conference Proceedings*, Vol. 45, pp. 109-112, June 8, 1976, propose the concept of a public key cryptosystem that would eliminate the need for a secure channel by making the sender's keying information public. It is also proposed how such a public key cryptosystem could allow an authentication system which generates an unforgeable message dependent digital signature. Diffie presents the idea of using a pair of keys E and D, for enciphering and deciphering a message, such that E is public information while D is kept secret by the intended receiver. Further, although D is determined by E, it is infeasible to compute D from E. Diffie suggests the plausibility of designing such a public key cryptosystem that would allow a user to encipher a message and send it to the intended receiver, but only the intended receiver could decipher it. While suggesting the plausibility of designing such systems, Diffie presents neither proof that public key cryptosystems exist, nor a demonstration system.

Diffie suggests three plausibility arguments for the existence of a public key cryptosystem; a matrix approach, a machine language approach and a logic mapping approach. While the matrix approach can be designed with matrices that require a demonstrably infeasible cryptanalytic time (i.e., computing D from E) using known methods, the matrix approach exhibits a lack of practical utility because of the enormous dimensions of the required matrices. The machine language approach and logic mapping approach are also suggested, but there is not way shown to design them in such a manner that they would require demonstrably infeasible cryptanalytic time.

Diffie also introduces a procedure using the proposed public key cryptosystems, that could allow the receiver to easily verify the authenticity of a message, but which prevents him from generating apparently authenticated messages. Diffie describes a protocol to be followed to obtain authentication with the proposed public key

cryptosystem. However, the authentication procedure relies on the existence of a public key cryptosystem which Diffie did not provide.

SUMMARY AND OBJECTS OF THE INVENTION

Accordingly, it is an object of this invention to allow authorized parties to a conversation (conversers) to converse privately even though an unauthorized party (eavesdropper) intercepts all of their communications.

Another object of this invention is to allow conversers on an insecure channel to authenticate each other's identity.

An illustrated embodiment of the present invention describes a method for communicating securely over an insecure channel without prearrangement of a cipher key. A secure cipher key is generated from transformations of exchanged transformed signals, which exchanged transformed signals are easy to effect but difficult to invert. The generated secure cipher key is used to encipher and decipher messages transmitted over the insecure communication channel.

This illustrated embodiment of the present invention describes a method and apparatus for generating a secure cipher key for use with conventional cryptographic communication between conversers over an insecure channel. The illustrated embodiment differs from a public key cryptosystem in that it provides a secure cipher key that is used with a conventional cryptographic system; a public key cryptosystem does not require a conventional cryptographic system. Further, the illustrated embodiment provides a means of transforming a signal that is practical to implement and is demonstrably infeasible to invert using known methods.

In the present invention a first converser transforms, in a manner infeasible to invert, a first signal while a second converser transforms, also in a manner infeasible to invert, a second signal. The first converser transmits the transformed first signal to the second converser, keeping the first signal secret, and the second converser transmits the transformed second signal to the first converser, keeping the second signal secret. The first converser then transforms the first signal with the transformed second signal to generate a third signal, representing a secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal. And, the second converser transforms the second signal with the transformed first signal to generate a fourth signal, also representing the secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal.

Another illustrated embodiment of the present invention describes a method for allowing a converser to authenticate another converser's identity. A first converser transforms, in a manner infeasible to invert, a first signal while a second converser transforms, also in a manner infeasible to invert, a second signal. The second converser places the transformed second signal in a public directory as the second converser's means of identification, keeping the second signal secret. The first converser transmits the transformed first signal to the second converser, with whom the first converser desires to communicate, keeping the first signal secret. The first converser then transforms the first signal with the second converser's transformed second signal, obtained from the public directory, to generate a third signal. The third signal represents a secure cipher key to

be used for conventional cryptographic communication with the second converter, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal. The second converter transforms the second signal with the transformed first signal to generate a fourth signal, also representing the secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal. The second converter's identity is authenticated by the first converter by the second converter's ability to generate the fourth signal, representing the secure cipher key, and to use the secure cipher key in communicating over a conventional cryptographic system.

Additional objects and features of the present invention will appear from the description that follows wherein the preferred embodiments have been set forth in detail in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a cryptographic system that transmits a computationally secure cryptogram over an insecure communication channel.

FIG. 2 is a block diagram of a secure key generator for raising various numbers to various powers in modulo arithmetic.

FIG. 3 is a block diagram of a multiplier for performing multiplications in the secure key generator of FIG. 2.

FIG. 4 is a detailed schematic diagram of an adder for performing additions in the multiplier of FIG. 3.

FIG. 5 is a detailed schematic diagram of a comparator for performing magnitude comparisons in the multiplier of FIG. 3.

FIG. 6 is a detailed schematic diagram of a subtractor for performing subtractions in the multiplier of FIG. 3.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to FIG. 1, a cryptographic system is shown in which all communications take place over an insecure communication channel 19, for example a telephone line. Two-way communication is exchanged on the insecure channel 19 between converter 11 and converter 12 using transmitter/receivers 31 and 32, for example modems such as Bell 210 modems. Converter 11 possesses an unenciphered or plaintext message P to be communicated to converter 12. Converter 11 and converter 12 include cryptographic devices 15 and 16 respectively, for enciphering and deciphering information under the action of a cipher key K on line K. For example, the cryptographic devices 15 and 16 may include the recently adopted National Data Encryption Standard. The cryptographic devices 15 and 16 implement transformations S_K and S_K^{-1} (the transformation which is the inverse of S_K) when loaded with key K. For example, key K may be a sequence of random letters or digits. The cryptographic device 15 enciphers the plaintext message P into an enciphered message or ciphertext C on line C that is transmitted by converter 11 through the insecure channel 19; the ciphertext C is received by converter 12 and deciphered by cryptographic device 16 to obtain the plaintext message P. An unauthorized party or eavesdropper 13 is assumed to have a cryptographic device 17 and to have access to the insecure channel 19, so if he knew the key K he could decipher the ciphertext C to obtain the plaintext message P.

Converter 11 and converter 12 include independent key sources 25 and 26 respectively, which generate numbers or signals that represent numbers. For example, the key sources may be random number generators that are implemented from noisy amplifiers (e.g., Fairchild $\mu 709$ operational amplifiers) with a polarity detector. Key source 25 generates three signals, q, a, and X_1 , and key source 26 generates X_2 ; a, X_1 and X_2 may be signals that represent independent random numbers chosen uniformly from the set of integers $(1, 2, \dots, q-1)$. Signals q and a are transmitted to the secure key generator 21 and are transmitted through the insecure channel 19 to secure key generator 22. Signals X_1 and X_2 are kept secret by converter 11 and converter 12 respectively, are given to the secure key generators 21 and 22 respectively, but are not transmitted through the insecure channel 19.

Converter 11 and converter 12 also include secure key generators 21 and 22 respectively, which accept the signals generated by the respective key sources 25 and 26. Secure key generator 22 also receives the signals q and a which are transmitted through the insecure channel 19. The secure key generators 21 and 22 generate signals Y_1 and Y_2 respectively by transforming X_1 and X_2 respectively with signals q and a in a manner that is easily performed but extremely difficult or infeasible to invert. A task is considered infeasible if its cost as measured by either the amount of memory used or the computing time is finite but impossibly large, for example, on the order of approximately 10^{30} operations with existing computational methods and equipment such transformations are characterized by the class of mathematical functions known as one-way cipher functions.

Signal Y_1 may be generated to represent the number obtained by raising the number represented by signal a to the power represented by signal X_1 , modulo the number represented by signal q; this transformation may be represented symbolically as $Y_1 = a^{X_1} \text{ mod } q$. Signal Y_2 may be generated to represent the number obtained by raising the number represented by signal a to the power represented by signal X_2 , modulo the number represented by signal q; this transformation may be represented symbolically as $Y_2 = a^{X_2} \text{ mod } q$.

Signals Y_1 and Y_2 are exchanged by transmitting Y_1 and Y_2 through the insecure channel 19 to secure key generators 22 and 21 respectively. Secure key generator 21 then generates a secure key K by transforming signal Y_2 with signals q, a and X_1 , and secure key generator 22 generates the same secure key K by transforming Y_1 with signals q, a and X_2 .

Secure key generator 21 may generate a secure key K represented by the number obtained by raising the number represented by signal Y_2 to the power represented by signal X_1 , modulo the number represented by signal q; this transformation may be represented symbolically as

$$K = Y_2^{X_1} \text{ mod } q = (a^{X_2})^{X_1} \text{ mod } q = a^{X_1 X_2} \text{ mod } q.$$

Secure key generator 22 may also generate the same secure key K represented by the number obtained by raising the number represented by signal Y_1 to the power represented by signal X_2 , modulo the number represented by signal q; this transformation may be represented symbolically as

$$K = Y_1^{X_2} \text{ mod } q = (a^{X_1})^{X_2} \text{ mod } q = a^{X_1 X_2} \text{ mod } q.$$

Conversers 11 and 12 then have the same secure key K which may be used with cryptographic devices 15 and 16.

The eavesdropper 13 is assumed to have a secure key generator 23 and to have access to all signals transmitted through the insecure channel 19, including signals q , a , Y_1 , and Y_2 . The difficulty of inverting the transformations which generated signals Y_1 and Y_2 make it infeasible for the eavesdropper 13 to generate signals X_1 or X_2 . Further, the secure key K is infeasible to generate solely with signals q , a , Y_1 and Y_2 .

The eavesdropper 13 is unable to compute the secure key K by multiplication or exponentiation; multiplication yields

$$Y_1 Y_2 = a^{X_1 + X_2} \bmod q \neq K$$

and exponentiation yields either

$$Y_1^{Y_2} = a^{(X_1 Y_2)} \neq K$$

or

$$Y_2^{Y_1} = a^{(X_2 Y_1)} \neq K$$

The eavesdropper in theory could obtain X_1 or X_2 from q , a and Y_1 and Y_2 by raising a to the first, second, third, etc., powers until Y_1 or Y_2 was obtained. This is prevented by choosing q to be a large number; if q is a 200 bit quantity, the average number of trials before success is on the order of $2^{199} = 4 \times 10^{59}$ and is physically infeasible. Improved algorithms for computing logarithms modulo q (if $Y = a^X \bmod q$, X is the logarithm of Y to the base a modulo q) are known but, if $q = 2r + 1$ with q and r being prime, then the most efficient known algorithm requires approximately q^2 operations. Again, taking $q = 2^{200}$, about $2^{100} = 10^{30}$ operations are required, still physically infeasible. An example of such a paid is $r = (2^{121} 5^2 7^2 11^2 13 17 19 23 29 31 37 41 43 47 53 59) + 1$ and $q = 2r + 1$. Other restrictions on q , a , X_1 and X_2 may also be imposed.

The secure key generators 21 and 22, for raising various numbers to various powers modulo q , can be implemented in electronic circuitry as shown in FIG. 2. For ease of illustration, FIG. 2 depicts raising a to the X power modulo q ; raising Y to the X power modulo q is obtained by initially loading Y , instead of a , into the A register 43.

FIG. 2 shows the initial contents of three registers 41, 42 and 43. The binary representation of X ($x_{k-1} x_{k-2} \dots x_1 x_0$) is loaded into the X register 41; 1 is loaded into the R register 42; and, the binary representation of a is loaded into the A register 43, corresponding to $i=0$. The number of bits k in each register is the least integer such that $2^k \geq q$. If $k=200$, then all three registers can be obtained from a single 1024 bit random access memory (RAM) such as the Intel 2102. The implementation of multiplier 44, for multiplying two numbers modulo q , will be described in more detail later.

Referring to FIG. 2, if the low order bit, containing x_0 , of the X register 41 equals 1 then the R register 42 and the A register 43 contents are multiplied modulo q and their product, also a k bit quantity, replaces the contents of the R register 42. If $x_0=0$, the R register 42 contents are left unchanged. In either case, the A register 43 is then loaded twice into the multiplier 44 so that the square, modulo q , of the A register 43 contents is computed. This value, $a^{(2^{i+1})}$, replaces the contents of

the A register 43. The X register 41 contents are shifted one bit to the right and a 0 is shifted in at the left so its contents are now $0x_{k-1} x_{k-2} \dots x_2 x_1$.

The low order bit, containing x_1 , of the X register 41 is examined. If it equals 1 then, as before, the R register 42 and A register 43 contents are multiplied modulo q and their product replaces the contents of the R register 42. If the low order bit equals 0 then the R register 42 contents are left unchanged. In either case, the contents of the A register 43 are replaced by the square, modulo q , of the previous contents. The X register 41 contents are shifted one bit to the right and a 0 is shifted in at the left so its contents are now $00x_{k-1} x_{k-2} \dots x_3 x_2$.

This process continues until the X register 41 contains all 0's, at which point the value of a^X modulo q is stored in the R register 42.

An example is helpful in following this process. Taking $q=23$, we find $k=5$ from $2^k \geq q$. If $a=7$ and $X=18$ then

$a^X = 7^{18} = 1,628,413,597,910,449 = 23(70,800,591,213,497) + 18$ so a^X modulo q equals 18. This straightforward but laborious method of computing a^X modulo q is used as a check to show that the method of FIG. 2, shown below, yields the correct result. The R register 42 and A register 43 contents are shown in decimal form to facilitate understanding.

i	X (in binary)	R	A
0	10010	1	7
1	01001	1	3
2	00100	3	9
3	00010	3	12
4	00001	3	6
5	00000	18	13

The row marked $i=0$ corresponds to the initial contents of each register, $X=18$, $R=1$ and $A=a=7$. Then, as described above, because the right most bit of X register 41 is 0, the R register 42 contents are left unchanged, the contents of the A register 43 are replaced by the square, modulo 23, of its previous contents ($7^2=49=2 \times 23 + 3=3$ modulo 23), the contents of the X register 41 are shifted one bit to the right, and the process continues. Only when $i=1$ and 4 do the right-most bit of the X register 41 contents equal 1, so only going from $i=1$ to 2 and from $i=4$ to 5 is the R register 42 replaced by RA modulo q . When $i=5$, $X=0$ so the process is complete and the result, 18, is in the R register 42.

Note that the same result, 18, is obtained here as in the straightforward calculation of 7^{18} modulo 23, but that here large numbers never resulted.

Another way to understand the process is to note that the A register contains a , a^2 , a^4 , a^8 and a^{16} when $i=0, 1, 2, 3$ and 4 respectively, and that $a^{18} = a^{16} a^2$, so only these two values need to be multiplied.

FIG. 3 continues the description of this illustrative implementation by depicting an implementation of the modulo q multiplier 44 in FIG. 2. The two numbers, y and z , to be multiplied are loaded into the Y and Z registers 51 and 52 respectively, and q is loaded in the Q register 53. The product yz modulo q will be produced in the P register 54 which is initially set to 0. If $k=200$, then all four registers can be obtained from a single 1024 bit RAM such as the Intel 2102. The implementation of FIG. 3 is based on the fact that $y z \bmod q = y_0 z_0 \bmod q + 2y_1 z_0 \bmod q + 4y_2 z_0 \bmod q + \dots + 2^{k-1} y_{k-1} z_0 \bmod q$.

where $y_k-1y_k-2 \dots y_1y_0$ is the binary representation of Y.

To multiply y times z, if the rightmost bit, containing y_0 , of the Y register 51 is 1 then the contents of the Z register 53 are added to the P register 54 by adder 55. If $y_0=0$, then the P register 54 is unchanged. Then the Q and P register contents are compared by comparator 56 to determine if the contents of the P register 54 are greater than or equal to q, the contents of the Q register 53. If the contents of the P register 54 are greater than or equal to q then subtractor 57 subtracts q from the contents of the P register 54 and places the difference in the P register 54, if less than q the P register 54 is unchanged.

Next, the contents of Y register 51 are shifted one bit to the right and a 0 is shifted in at the left so its contents become $0y_k-1y_k-2 \dots y_2y_1$, so that y_1 is ready for computing $2yz \bmod q$. The quantity $2z \bmod q$ is computed for this purpose by using adder 55 to add z to itself, using comparator 56 to determine if the result, $2z$, is less than q, and using subtractor 57 for subtracting q from $2z$ if the result is not less than q. The result, $2z \bmod q$ is then stored in the Z register 52. The rightmost bit, containing y_1 , of the Y register 51 is then examined, as before, and the process repeats.

This process is repeated a maximum of k times or until the Y register 51 contains all 0's, at which point $xy \bmod q$ is stored in the P register 54.

As an example of these operations, consider the problem of computing $7 \times 7 \bmod 23$ needed to produce the second state of the A register when $7^{18} \bmod 23$ was computed. The following steps show the successive contents of the Y, Z and P registers which result in the answer $7 \times 7 = 3 \bmod 23$.

i	Y (in binary)	Z	P
0	00111	7	0
1	00011	14	$0 + 7 = 7$
2	00001	5	$7 + 14 = 21$
3	00000	10	$21 + 5 = 3 \bmod 23$

FIG. 4 depicts an implementation of an adder 55 for adding two k bit numbers p and z. The numbers are presented one bit at a time to the device, low order bit first, and the delay element is initially set to 0. (The delay represents the binary carry bit.) The AND gate 61 determines if the carry bit should be a one based on p_i and z_i both being 1 and the AND gate 62 determines if the carry should be a 1 based on the previous carry being a 1 and one of p_i or z_i being 1. If either of these two conditions is met, the OR gate 63 has an output of 1 indicating a carry to the next stage. The two exclusive-or (XOR) gates 64 and 65 determine the i^{th} bit of the sum, s_i , as the modulo-2 sum of p_i , z_i and the carry bit from the previous stage. The delay 66 stores the previous carry bit. Typical parts for implementing these gates and the delay are SN7400, SN7404, and SN7474.

FIG. 5 depicts an implementation of a comparator 56 for comparing two numbers p and q. The two numbers are presented one bit at a time, high order bit first. If neither the $p < q$ nor the $p > q$ outputs have been triggered after the last bits p_0 and q_0 have been presented, then $p = q$. The first triggering of either the $p < q$ or the $p > q$ output causes the comparison operation to cease. The two AND gates 71 and 72 each have one input inverted (denoted by a circle at the input). An SN7400 and SN7404 provide all of the needed logic circuits.

FIG. 6 depicts an implementation of a subtractor 57 for subtracting two numbers. Because the numbers subtracted in FIG. 3 always produce a non-negative difference, there is no need to worry about negative differences. The larger number, the minuend, is labelled p and the smaller number, the subtrahend, is labelled q. Both p and q are presented serially to the subtractor 57, low order bit first. AND gates 81 and 83, OR gate 84 and XOR gate 82 determine if borrowing (negative carrying) is in effect. A borrow occurs if either $p_i=0$ and $q_i=1$, or $p_i=q_i$ and borrowing occurred in the previous stage. The delay 85 stores the previous borrow state. The i^{th} bit of the difference, d_i , is computed as the XOR, or modulo-2 difference, of p_i , q_i , and the borrow bit. The output of XOR gate 82 gives the modulo-2 difference between p_i and q_i , and XOR gate 86 takes the modulo-2 difference of this with the previous borrow bit. Typical parts for implementing these gates and the delay are SN7400, SN7404 and SN7474.

There are many methods for implementing this form of the invention. The signals q and a may be public knowledge rather than generated by the key source 25. Further, it should be appreciated that the present invention has the capability of being modified by the use of additional transformations or exchanges of signals.

In some applications, it will prove valuable to have the i^{th} converter on the system generate Y_i as above and place it in a public file or directory rather than transmitting it to another converter with whom he wishes to communicate. Then two converters i and j who wish to establish a secure channel will use $K_{ij} = Y_i^{A_j} \bmod q = Y_j^{A_i} \bmod q$ as their key. The advantage is that converter i, having once proved his identity to the system through the use of his driver's license, fingerprint, etc., can prove his identity to converter j by his ability to compute K_{ij} and encrypt data with it.

Variations on the above described embodiment are possible. For example, in the above method based on logarithms modulo q, m-dimensional vectors, each of whose components are between 0 and q-1 could also be used. Then all operations are performed in the finite field with q^m elements, which operations are well described in the literature. Thus, although the best mode contemplated for carrying out the present invention has been herein shown and described, it will be apparent that modification and variation may be made without departing from what is regarded to be the subject matter of this invention.

What is claimed is:

1. A secure key generator comprising:

- a first input connected to receive an applied first signal;
- a second input connected to receive an applied second signal;
- a first output;
- a second output; and

means for generating at the first output a third signal, that is a transformation of said first signal and which transformation is infeasible to invert, and for generating at the second output a fourth signal, that is a transformation of said second signal with said first signal, which represents a secure key and is infeasible to generate solely with said second signal and said third signal.

2. In a method of communicating securely over an insecure communication channel of the type which communicates a message from a transmitter to a receiver, the improvement characterized by:

generating and transforming, in a manner infeasible to invert, a first signal at the transmitter to generate a transformed first signal;
 generating and transforming, in a manner infeasible to invert, a second signal at the receiver to generate a transformed second signal;
 transmitting said transformed first signal from the transmitter to the receiver;
 transmitting said transformed second signal from the receiver to the transmitter;
 transforming said transformed second signal with said first signal at the transmitter to generate a third signal, representing a secure cipher key, that is infeasible to generate solely with said transformed first signal and said transformed second signal;
 transforming said transformed first signal with said second signal at the receiver to generate a fourth signal that is identical to the third signal and represents said secure cipher key;
 enciphering the message with said secure cipher key at the transmitter;
 transmitting the enciphered message from the transmitter to the receiver; and
 deciphering the enciphered message with said secure cipher key at the receiver.

3. In a method of communicating securely over an insecure communication channel as in claim 2, further comprising:
 authenticating the receiver's identity at the transmitter from the receiver's ability to generate the fourth signal, representing the secure cipher key.

4. A method of generating a secure cipher key between a transmitter and receiver comprising the steps of:
 generating and transforming, in a manner infeasible to invert, a first signal at the transmitter to generate a transformed first signal;
 generating and transforming, in a manner infeasible to invert, a second signal at the receiver to generate a transformed second signal;
 transmitting said transformed first signal from the transmitter to the receiver;
 transmitting said transformed second signal from the receiver to the transmitter;
 transforming said transformed second signal with said first signal at the transmitter to generate a third signal, representing a secure cipher key, that is infeasible to generate solely with said transformed first signal and said transformed second signal; and
 transforming said transformed first signal with said second signal at the receiver to generate a fourth signal that is identical to the third signal and represents said secure cipher key.

5. An apparatus for generating a secure cipher key comprising:
 a first secure key generator having a first input connected to receive an applied first signal, having a second input connected to receive a second signal, having a first and second outputs, and having a means for generating at the first output a third signal, that is a transformation of said first signal and which transformation is infeasible to invert, and for generating at the second output a fourth signal, that is a transformation of said second signal with said first signal, which represents a secure key and is infeasible to generate solely with said second signal and said third signal; and

a second secure key generator having a first input connected to receive an applied fifth signal, having a second input connected to receive said third signal, having a first and second outputs, and having a means for generating at the first output said second signal, that is a transformation of said fifth signal and which transformation is infeasible to invert, and for generating at the second output a sixth signal, that is a transformation of said third signal with said fifth signal, which represents the secure key and is infeasible to generate solely with said second signal and said third signal.

6. A method of generating a secure cipher key between a transmitter and receiver comprising the steps of:
 transforming, in a manner infeasible to invert, a first signal at the transmitter to generate a transformed first signal wherein transforming said first signal is performed by raising a first number to a power represented by said first signal, modulo a second number;
 transforming, in a manner infeasible to invert, a second signal at the receiver to generate a transformed second signal, wherein transforming said second signal is performed by raising the first number to a power represented by said second signal, modulo the second number;
 transmitting said transformed first signal from the transmitter to the receiver;
 transmitting said transformed second signal from the receiver to the transmitter;
 transforming said transformed second signal with said first signal at the transmitter to generate a third signal, representing a secure cipher key, that is infeasible to generate solely with said transformed first signal and said transformed second signal, wherein transforming said transformed second signal with said first signal is performed by raising a number represented by said transformed second signal to a power represented by said first signal, modulo the second number; and
 transforming said transformed first signal with said second signal at the receiver to generate a fourth signal, representing said secure cipher key, that is infeasible to generate solely with said transformed first signal and said transformed second signal, wherein transforming said transformed first signal with said second signal is performed by raising a number represented by said transformed first signal to a power represented by said second signal, modulo the second number.

7. An apparatus for generating a secure cipher key comprising:
 a first secure key generator having a first input connected to receive an applied first signal, having a second input connected to receive a second signal, having first and second outputs, and having a means for generating at the first output a third signal, that is a transformation of said first signal in which said transformation includes raising a first number to a power represented by said first signal, modulo or second number, and for generating at the second output a fourth signal, that is a transformation of said second signal with said first signal which transformation includes raising a number represented by said second signal to a power represented by said first signal, modulo the second number, which represents a secure key and is infeasible

11

to generate solely with said second signal and said third signal; and

- a second secure key generator having a first input connected to receive an applied fifth signal, having a second input connected to receive said third signal, having a first and second outputs, and having a means for generating at the first output said second signal, that is a transformation of said fifth signal in which said transformation includes raising a first number to a power represented by said fifth signal, modulo the second number, and for generating at the second output a sixth signal, that is a transformation of a said third signal with said fifth signal which transformation includes raising a number represented by said third signal to a power represented by said fifth signal, modulo the second number, which represents the secure key and is infeasible to generate solely with said second signal and said third signal.

8. An apparatus for generating a secure cipher key comprising:

- a first secure key generator having a first input connected to receive an applied first signal, having a second input connected to receive a second signal, having a first and second outputs, and having a means for generating at the first output a third signal, said third signal Y_i being described by

$$Y_i = a^{x_i} \bmod q$$

where

q = a large prime number

a = a random number, such that $1 \leq a \leq q-1$

x_i = the first signal which represents a random number, such that $1 \leq x_i \leq q-1$

12

a transformation of said first signal which is infeasible to invert, and for generating at the second output a fourth signal, said fourth signal K_j being described by

$$K_j = Y_j^{x_j} \bmod q$$

where

Y_j = the second signal

a transformation of said second signal with said first signal, which represents said secure cipher key and is infeasible to generate solely with said second signal and said third signal; and

- a second secure key generator having a first input connected to receive an applied fifth signal, having a second input connected to receive said third signal, having a first and second outputs, and having a means for generating at the first output a second signal, said second signal Y_j being described by

$$Y_j = a^{x_j} \bmod q$$

where

x_j = the fifth signal which represents a random number, such that $1 \leq x_j \leq q-1$

a transformation of said fifth signal which is infeasible to invert, and for generating at the second output a sixth signal, said sixth signal K_j being described by

$$K_j = Y_j^{x_j} \bmod q$$

a transformation of said third signal with said fifth signal, which represents the secure key and is infeasible to generate solely with said second signal and said third signal.

* * * * *

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. V. Stambler

DATE: 12/14/98



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Attn: Drawing Review
Leon Stambler : Branch
:
Appln. No.: 08/872,116 : Group Art Unit: 2735
:
Filed: June 10, 1997 : Examiner: B. Zimmerman
:
For: METHOD FOR SECURING :
INFORMATION RELEVANT TO A : Attorney Docket
TRANSACTION (as amended) : No. 6074-1U7

COPY

TRANSMITTAL OF FORMAL DRAWINGS
PRIOR TO NOTICE OF ALLOWANCE

Attached please find the formal drawings for this application consisting of fifteen sheets of drawings, Figs. 1-16. The formal drawings incorporate the changes in the "SUBMISSION OF PROPOSED DRAWING AMENDMENT FOR APPROVAL BY EXAMINER" mailed on November 8, 1996 (filed in the USPTO on November 13, 1996) and the "SUBMISSION OF PROPOSED DRAWING AMENDMENT FOR APPROVAL BY EXAMINER" mailed on July 21, 1998 (filed in the USPTO on July 23, 1998), both of which were previously approved by the Examiner.

Respectfully submitted,

LEON STAMBLER

12/14/98
(Date)

BY:

Clark A. Jablon

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



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

DATE: 12/14/98

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit: 2735
Leon Stambler :
Appln. No.: 08/872,116 : Examiner: B. Zimmerman
Filed: June 10, 1997 :
For: METHOD FOR SECURING :
INFORMATION RELEVANT TO A : Attorney Docket
TRANSACTION (as amended) : No. 6074-1U7

RECEIVED

DEC 24 1998

Group 2700

RESPONSE

This paper is being filed in response to the Office Action mailed September 15, 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 statutory disclaimer fee for presenting the terminal disclaimer.

 **PALM INTRANET**3-2
Day : Monday
Date: 4/ 5/1999
Time: 09:33:18**PUBS Application Status Query for 08/872116****View Work Flow Content**

Search Another: Serial Number

 Search

Class/Subclass : 340/825.330

Status : 093/ALLOWED - NOTICE OF ALLOWANCE MAILED - RELEASED TO OFFICE OF PUBLICATIONS

Location : 7560/ ALLOWED FILES 305-8495

Charge to Location : /

Potential Issue Ready No

Requirements Needed

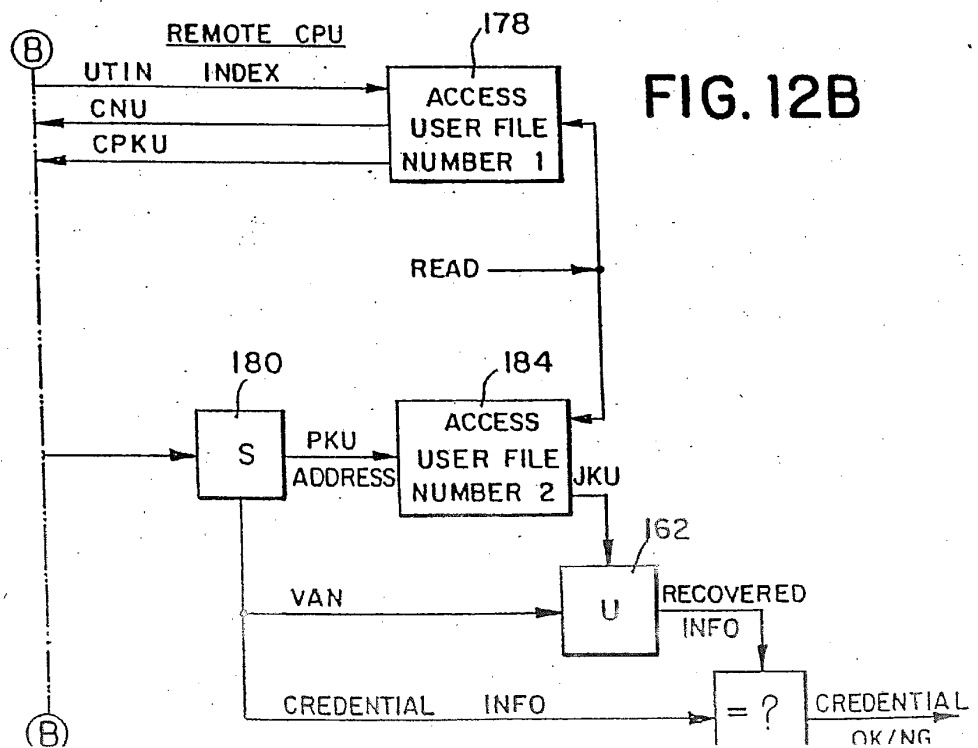
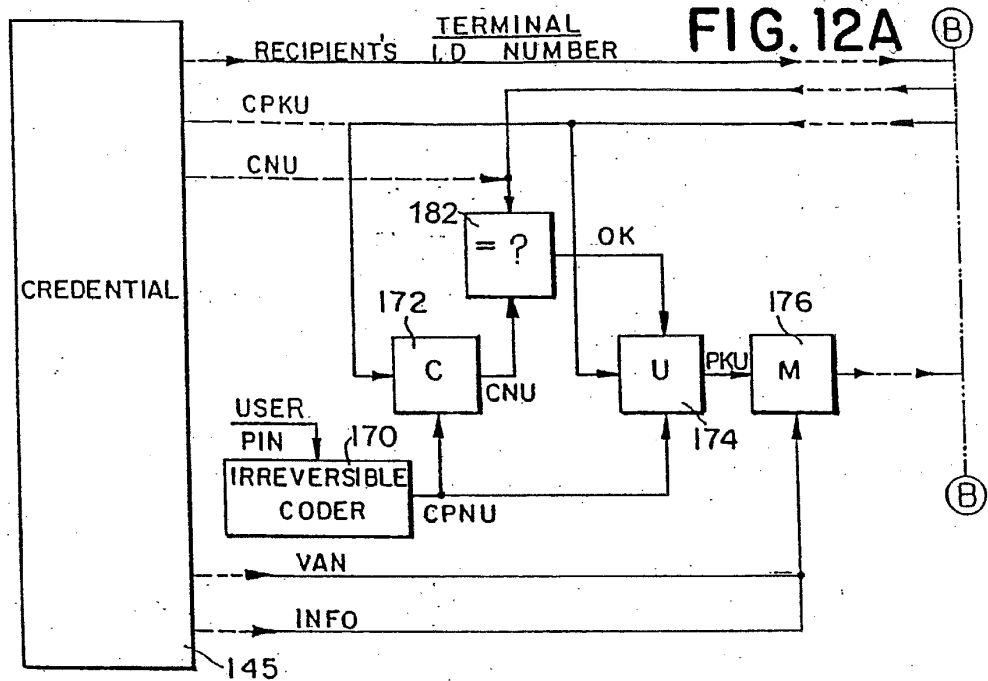
Drawing Required	Yes
Issue Fee Required	Yes
On Query	No
85B Required	Yes
PUBS Unmatched Paper	No
Unmatched Petition	No
Biotech	No
Petition	No
PCT	No
Needs Panel Review at TC	No
Under Quality Review	No

Go BACK Use BACK Button on Your BROWSER Tool Bar)

Back to || [PUBS](#) || [PALM](#) || [OASIS](#) || Home Page

4/5/99 9:35 AM

STAM0041715





PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-IU7

SHEET NO. 6 OF 15

RECEIVED
APR 15 1999
Publishing
Comm

STAM0041717

REDEEMER BANK CPU





PANITCH SCHWARZE JACOBS & NADEL, P.C.

INTELLECTUAL PROPERTY ATTORNEYS
ONE COMMERCE SQUARE
2005 MARKET STREET, 22ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103-7086

TELEPHONE: (215) 567-2020

APPLICANT: Leon Stambler

APPLN. NO.: 08/872,116

FILED: June 10, 1997

TITLE: METHOD FOR SECURING INFORMATION RELEVANT TO A
TRANSACTION (as amended)

ATTORNEY DOCKET NO.: 6074-1U7

SHEET NO. 8 OF 15

RECEIVED

APR 15 1999

Publishing Co.

STAM0041719

Deposit Account Maintenance

Deposit Account Window Help

Print Screen

Deposit Account Number: 1160235 Balance Amount: -18,741

Holder Name: PANITCH SCHWARZE JACOBS & NADEL

Address:

Attention: DAVID STAUB

Street: ONE COMMERCE SQUARE

2005 MARKET STREET, 22ND FLOOR

Province:

City: PHILADELPHIA

State: PA Postal Code: 19103-7086

Country: US

Telephone: 215-567-2020 Fax: 215-567-2991

Details:

Category Code: NONGOVNMNT Type: REGULAR

Notification Amt: 0.00 Status: ☒ Active ☐ Closed

Access Code: 9434

Taskbar: PIN/0000 welcome to Calculator Deposit A 8:57 AM

5-7-99

STAM0041720

United States Patent [19]

Riek et al.

[11] Patent Number: 5,054,066

[45] Date of Patent: Oct. 1, 1991

[54] ERROR CORRECTING PUBLIC KEY
CRYPTOGRAPHIC METHOD AND
PROGRAM

[75] Inventors: Justus Riek, Glen Cove; Gregory
McFarland, Port Jefferson, both of
N.Y.

[73] Assignee: Grumman Corporation, Bethpage,
N.Y.

[21] Appl. No.: 272,502

[22] Filed: Nov. 16, 1988

[51] Int. Cl.³ H04L 9/30

[52] U.S. Cl. 380/30; 380/50

[58] Field of Search 380/21, 30, 50

[56] References Cited

U.S. PATENT DOCUMENTS

4,165,444	8/1979	Gordon	380/50
4,200,770	4/1980	Hellman et al.	380/30
4,208,739	6/1980	Lu et al.	380/28
4,218,582	8/1980	Hellman et al.	380/30
4,306,111	12/1981	Lu et al.	380/30
4,351,982	9/1982	Miller et al.	380/30
4,417,338	11/1983	Davida	380/21
4,424,414	1/1984	Hellman et al.	380/30
4,514,592	4/1985	Miyaguchi	380/30

4,841,570 6/1989 Cooper 380/30

OTHER PUBLICATIONS

McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory", by R. J. McEliece, DSN Progress Report 42-44.

Riek et al., "Public Key Encryption and Computer Communications Security in SDI Networks", Aug. 5, 6, 7, 1986.

Diffie et al., "Privacy and Authentication: An Introduction to Cryptography", vol. 67, No. 3, Me. 1979, pp. 397-427.

Diffie et al., "Multiuser Cryptographic Techniques", vol. 45, Jun. 3, 1976, pp. 109-112.

Diffie et al., "New Directions in Cryptography", Nov. 1976, pp. 644-654.

Primary Examiner—Salvatore Cangialosi

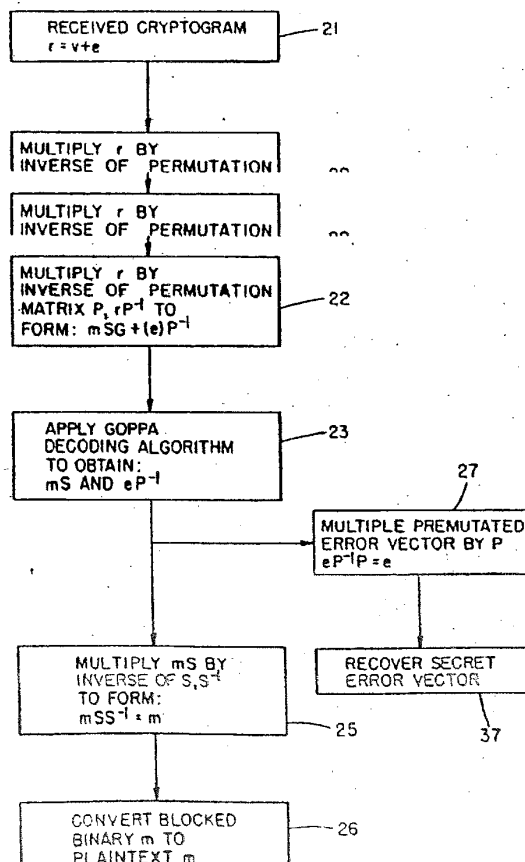
Attorney, Agent, or Firm—Scully, Scott, Murphy & Presser

[57]

ABSTRACT

The present invention relates to cryptographic systems, and particularly, public key cryptographic systems implemented in digital communication devices.

14 Claims, 5 Drawing Sheets



STAM0041721

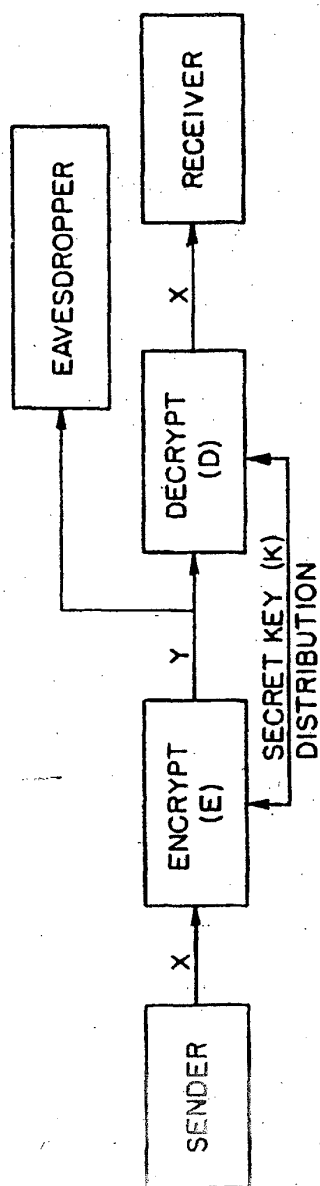


FIG. 1(a) PRIOR ART CONVENTIONAL CRYPTOGRAPHY PARADIGM

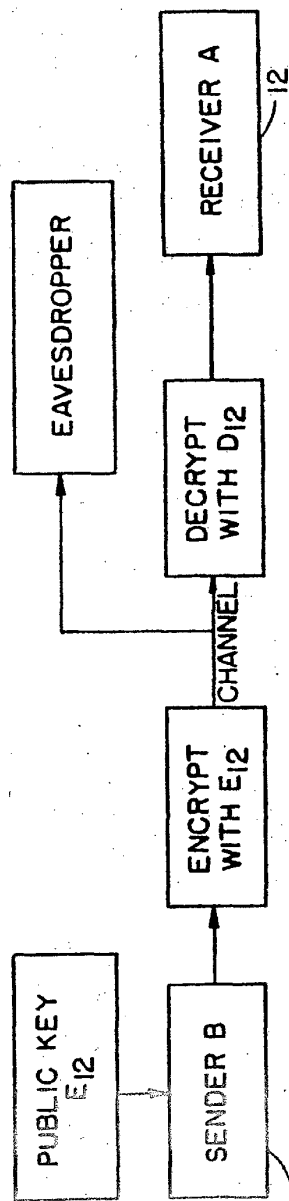


FIG. 1(b) PRIOR ART PUBLIC KEY CRYPTOGRAPH PARADIGM

Thus, it is clear that the original error vector itself is recoverable and can be used as a carrier of information.

I claim:

1. A method of transmitting a digital cryptogram over a communications channel by means of a public key algorithm, said method comprising:

- (a) constructing a first generator matrix with a preselected finite field and an irreducible Goppa polynomial, said polynomial providing a degree s error correcting capability,
- (b) constructing a scrambled generator matrix by matrix multiplication, said scrambled generator matrix being the product of a non-singular matrix, said first generator matrix and a permutation matrix,
- (c) converting plaintext message to be sent to binary form and blocking the message to a predetermined size, said size corresponding to the number of rows in said scrambled generator matrix, said blocked binary message forming a message vector,
- (d) encoding the message vector with the scrambled generator matrix using matrix multiplication to form a code vector,
- (e) adding a preselected error vector to the code vector in component wise fashion using modulo 2 arithmetic, to generate a cryptogram,
- (f) transmitting said cryptogram over a communications channel, said channel having a channel error probability, wherein the combined predetermined error vector and the channel error vector do not exceed the degree s error correcting capability.

2. A method of decoding a digital cryptogram, when the cryptogram was created with a public key scrambled generator matrix, said scrambled matrix being the product of a permutation matrix, a non-singular matrix, and a generator matrix formed from an irreducible Goppa polynomial, said method comprising:

- (a) multiplying a received cryptogram by the inverse of the permutation matrix used in creating the public key scrambled matrix to obtain a permuted form of the received cryptogram,
- (b) apply a Goppa decoding algorithm to the permuted form of the received cryptogram to find mS and a permuted error vector, wherein m represents the original message encoded and S represents the non-singular matrix
- (c) multiply mS by the inverse of the non-singular matrix to derive m , a binary form of a plaintext message
- (d) multiply the permuted error vector by the permutation matrix to derive a preselected error vector.

3. A method of transmitting a digital cryptogram over a communications channel as claimed in claim 1, wherein an authentication code is selected and added to the message as the preselected error vector.

4. A method of decoding a digital cryptogram as claimed in claim 2, wherein the received error vector is used to authenticate the sender of the cryptogram.

5. A method of transmitting a digital cryptogram over a communications channel as claimed in claim 1, wherein the communications channel is further defined to be a common carrier data link, said method further comprising the step of inserting a preselected error in any block of the cryptogram that exceeds a predetermined ones density requirement.

6. A method of transmitting a digital cryptogram over a communications channel as claimed in claim 1,

wherein the preselected error vector is chosen from an extended heavyweight error pattern.

7. A method of decoding a digital cryptogram as claimed in claim 2, wherein e is further defined as a heavyweight error pattern.

8. A method of transmitting a digital cryptogram over a communications channel by means of a public key algorithm, said method comprising:

- (a) constructing a first generator matrix with a preselected finite field and an irreducible Goppa polynomial, said polynomial providing a degree s error correcting capability,
- (b) constructing a scrambled generator matrix by matrix multiplication, said scrambled generator matrix being the product of a non-singular matrix, said first generator matrix and a permutation matrix,
- (c) converting plaintext message to be sent to binary form and blocking the message to a predetermined size, said size corresponding to the number of rows in said scrambled generator matrix, said blocked binary message forming a message vector,
- (d) encoding the message vector with the scrambled generator matrix using matrix multiplication to form a code vector,
- (e) adding a preselected heavy weight error vector to the code vector in component wise fashion using modulo 2 arithmetic, to generate a cryptogram.

9. A method of transmitting a digital cryptogram over a communications channel as claimed in claim 1, wherein the communications channel is further defined to be a common carrier data link, said method further comprising the step of inserting a preselected error in any block of the cryptogram that exceeds a predetermined ones density requirement.

10. A method of transmitting a digital cryptogram over a communications channel by means of a public key algorithm, said method comprising:

- (a) constructing a first generator matrix with a preselected finite field and an irreducible Goppa polynomial, said polynomial providing a degree s error correcting capability,
- (b) constructing a scrambled generator matrix by matrix multiplication, said scrambled generator matrix being the product of a non-singular matrix, said first generator matrix and a permutation matrix,
- (c) converting plaintext message to be sent to binary form and blocking the message to a predetermined size, said size corresponding to the number of rows in said scrambled generator matrix, said blocked binary message forming a message vector,
- (d) encoding the message vector with the scrambled generator matrix using matrix multiplication to form a code vector,
- (e) adding a preselected heavy weight error vector to the code vector in component wise fashion using modulo 2 arithmetic, to generate a cryptogram, said error vector including a secondary message.

11. A method of decoding a digital cryptogram, when the cryptogram was created with a public key scrambled generator matrix, said scrambled matrix being the product of a permutation matrix, a non-singular matrix, and a generator matrix formed from an irreducible Goppa polynomial, said method comprising:

- (a) multiplying a received cryptogram by the inverse of the permutation matrix used in creating the pub-

25

lic key scrambled matrix to obtain a permuted form of the received cryptogram.

(b) apply a Goppa decoding algorithm to the permuted form of the received cryptogram to find mS and a permuted error vector, wherein m represents the original message encoded and S represents the non-singular matrix,

(c) multiply mS by the inverse of the non-singular matrix to derive m , a binary form of a plaintext message,

(d) multiply the permuted error vector by the permutation matrix to derive a secondary message.

12. A method of transmitting a digital cryptogram over a communications channel as claimed in claim 10,

26

wherein an authentication code is selected and added to the message as a component of the secondary message.

13. A method decoding a digital cryptogram as claimed in claim 11, wherein the received error vector is used to authenticate the sender of the cryptogram.

14. A method of transmitting a digital cryptogram over a communications channel as claimed in claim 10, wherein the communications channel is further defined to be a common carrier data link, said method further comprising the step of inserting a preselected error in any block of the cryptogram that exceeds a predetermined ones density requirement.

* * * * *

15

20

25

30

35

40

45

50

55

60

65

-continued

$$r_{i-2}(x) = q_i(x)r_{i-1}(x) + r_i(x) \quad \deg r_i(x) < \deg r_{i-1}(x)$$

$$s_i(x) = s_{i-2}(x) - q_i(x)s_{i-1}(x)$$

$$t_i(x) = t_{i-2}(x) - q_i(x)t_{i-1}(x)$$

With the following initial conditions

$$s_{-1}(x) = 1 \quad t_{-1}(x) = 0 \quad r_{-1}(x) = G(x)$$

$$s_0(x) = 0 \quad t_0(x) = 1 \quad r_0(x) = R(x).$$

It is noted that several properties are associated with these recurrence relations.

Lemma 1: $s_i(x)t_{i-1}(x) - s_{i-1}(x)t_i(x) = (-1)^i + 1, 0 \leq i \leq n+1$.

Proof (by induction)

$$i = 0: s_0(x)t_{-1}(x) - s_{-1}(x)t_0(x) =$$

$$0 \cdot 0 - 1 \cdot 1 = -1 = (-1)^0 + 1.$$

assume for i .

prove for $i+1$: $s_{i+1}(x)t_i(x) - s_i(x)t_{i+1}(x) = (-1)^{i+1} + 1$.

But

$$s_{i+1}(x) = s_{i-1}(x) - q_{i+1}(x)s_i(x)$$

$$t_{i+1}(x) = t_{i-1}(x) - q_{i+1}(x)t_i(x).$$

Thus

$$[s_{i+1}(x) - q_{i+1}(x)s_i(x)]t_i(x) - s_i(x)[t_{i+1}(x) - q_{i+1}(x)t_i(x)] \quad \text{Q.E.D.}$$

=

$$s_{i+1}(x)t_i(x) - s_i(x)t_{i+1}(x) =$$

$$-(s_i(x)t_{i-1}(x) - s_{i-1}(x)t_i(x)) = -(-1)^i + 1 = (-1)^{i+1} + 1.$$

Lemma 2: $s_i(x)G(x) + t_i(x)R(x) = r_i(x), -1 \leq i \leq n+1$.

Proof (by induction)

$$i = -1: s_{-1}(x)G(x) + t_{-1}(x)R(x) =$$

$$1 \cdot G(x) + 0 \cdot R(x) = G(x) = r_{-1}(x).$$

assume for i .

prove for $i+1$: $s_{i+1}(x)G(x) + t_{i+1}(x)R(x) = r_{i+1}(x)$.

Substituting for

$s_{i+1}(x), t_{i+1}(x)$ and $r_{i+1}(x)$ we get

$$s_{i+1}(x)G(x) - q_{i+1}(x)s_i(x)G(x) + t_{i+1}(x)R(x) - q_{i+1}(x)t_i(x)R(x) =$$

$$[s_{i+1}(x)G(x) + t_{i+1}(x)R(x)] - q_{i+1}(x)[s_i(x)G(x) + t_i(x)R(x)] =$$

(by inductive assumption)

$$[r_{i+1}(x)] - q_{i+1}(x)[r_i(x)] = r_{i+1}(x).$$

Lemma 3: $\deg t_i(x) + \deg r_{i-1}(x) = \deg G(x), 0 \leq i \leq n+1$.

Proof (by induction)

Before beginning the formal inductive proof, one may prove a small result which will be needed in the inductive step.

Using the relation for $t_i(x)$,

note that

$$t_i(x) = t_{i-2}(x) - q_i(x)t_{i-1}(x), \text{ so that}$$

$$t_0(x) = 1$$

$$t_1(x) = t_{-1}(x) - q_1(x)t_0(x) = 0 - q_1(x)$$

$$t_2(x) = t_0(x) - q_2(x)t_1(x) = 1 + q_2(x)q_1(x)$$

$$t_3(x) = t_1(x) - q_3(x)t_2(x) = -q_1(x) - q_3(x)q_2(x)q_1(x)$$

.

etc.

Thus, in general,

Thus, in general,

$$\deg t_i(x) = \sum_{j=1}^i \deg q_j(x).$$

$i = 0$:

$$\deg t_0(x) + \deg r_{-1}(x) =$$

$$0 + \deg G(x) = \deg G(x).$$

assume for i .

prove for $i+1$: $\deg t_{i+1}(x) + \deg r_i(x) = \deg G(x)$.

Substituting, one finds

$$\deg t_{i+1}(x) = \deg[t_{i-1}(x) - q_{i+1}(x)t_i(x)] = \deg q_{i+1}(x)t_i(x)$$

since

$$\deg t_{i-1}(x) = \sum_{j=1}^{i-1} \deg q_j(x),$$

$$\deg q_{i+1}(x)t_i(x) = \sum_{j=1}^{i+1} \deg q_j(x)$$

and

$$\sum_{j=1}^{i-1} \deg q_j(x) \leq \sum_{j=1}^{i+1} \deg q_j(x).$$

Substituting again,

$$\deg r_i(x) = \deg \left[\frac{r_{i-1}(x) - r_{i+1}(x)}{q_{i+1}(x)} \right] = \deg \frac{r_{i-1}(x)}{q_{i+1}(x)}.$$

Thus

$$\deg t_{i+1}(x) + \deg r_i(x) =$$

$$15 \quad [\deg q_{i+1}(x)t_i(x)] + \left[\deg \frac{r_{i-1}(x)}{q_{i+1}(x)} \right] =$$

$$[\deg q_{i+1}(x) + \deg t_i(x)] + [\deg r_{i-1}(x) - \deg q_{i+1}(x)] =$$

$$20 \quad \deg t_i(x) + \deg r_{i-1}(x) = \deg G(x), \text{ by hypothesis}$$

Finally the following important lemma may be proved.

Lemma 4 With $G(x), R(x)$ defined as above, there exists a unique integer $i, 0 \leq i \leq n$ such that

$$25 \quad \deg t_i(x) \leq s - s/2 - 1, \quad \deg G(x) = s$$

$$\deg r_i(x) \leq s/2 \quad x = \text{greatest integer function}$$

Proof

Recall that both $\deg r_i(x)$ and $\deg t_i(x)$ are strictly decreasing and increasing sequences, respectively. One may define i by requiring that

$$35 \quad \deg r_{i-1}(x) \leq s/2 + 1$$

$$\deg t_i(x) \leq s/2.$$

There can be only one such value for i . Then, by Lemma 3

$$\deg t_i(x) + \deg r_{i-1}(x) = \deg G(x) = s,$$

which implies that

$$45 \quad \deg t_i(x) \leq s - s/2 - 1$$

$$\deg t_{i+1}(x) \leq s/2.$$

Again, there can be only one such value for i . Q.E.D.

With the foregoing one may now prove the most important result.

Theorem

Given the equivalence relation

$$60 \quad \beta(x)R(x) = \alpha(x) \bmod G(x), \quad \deg \beta(x) \leq \frac{s-1}{2} \\ \deg \alpha(x) \leq s/2$$

there is a unique i such that

$$65 \quad \beta(x) = t_i(x)$$

$$\alpha(x) = r_i(x).$$

Proof

One separates the proof into two parts. (Part 1) Suppose that one assumes, for the moment, that

$$\begin{aligned}\beta(x) &= t_i(x) \\ \alpha(x) &= r_i(x), \text{ for some } i\end{aligned}$$

It may be shown that i is unique.

Re-write the restrictions on the degrees of the polynomials $\alpha(x)$ and $\beta(x)$ using the greatest integer functions:

$$\deg \alpha(x) \leq \frac{s}{2}$$

$$\deg \beta(x) \leq \frac{s-1}{2}$$

But

$$\frac{s}{2} + \frac{s-1}{2} = s-1,$$

so that

$$\frac{s-1}{2} = s - \frac{s}{2} - 1$$

and it is seen that

$$\deg \alpha(x) \leq s/2 \text{ ps}$$

$$\deg \beta(x) \leq s - s/2 - 1,$$

the upper bounds from Lemma 4.

Thus, on the assumption that some index i exists such that

$$\beta(x) = t_i(x)$$

$$\alpha(x) = r_i(x), \text{ the index is unique}$$

since

$$\deg \beta(x) = \deg t_i(x) \leq s - s/2 - 1$$

$$\deg \alpha(x) = \deg r_i(x) \leq s/2$$

(Part 2) Using Lemma 2 and $\beta(x)R(x) - \alpha(x) \bmod G(x)$ one may write the following equations

$$\begin{aligned}s_i(x)G(x) + t_i(x)R(x) &= r_i(x) \\ s_i(x)G(x) + \beta(x)R(x) &= \alpha(x), \text{ for some } s_i(x).\end{aligned} \quad (1)$$

Multiplying by $\beta(x)$ and $t_i(x)$ respectively one obtains

$$\begin{aligned}\beta(x)s_i(x)G(x) + \beta(x)t_i(x)R(x) &= \beta(x)r_i(x) \\ t_i(x)s_i(x)G(x) + t_i(x)\beta(x)R(x) &= t_i(x)\alpha(x).\end{aligned} \quad (2)$$

But this implies that

$$\beta(x)s_i(x)G(x) - t_i(x)s_i(x)G(x) = \beta(x)r_i(x) - t_i(x)\alpha(x)$$

or, equivalently

$$\beta(x)r_i(x) = t_i(x)\alpha(x) \bmod G(x).$$

Examining the degrees of both sides of this equivalence shows

$$\deg \beta(x) + \deg r_i(x) \leq s - 1 + s/2 < s$$

$$\deg t_i(x) + \deg \alpha(x) \leq s - 2 + 1 + s/2 < s,$$

so the equivalence is an equality:

$$\beta(x)r_i(x) = t_i(x)\alpha(x).$$

Substituting back into the same pair of equations (2) we see that this implies

$$\beta(x)s_i(x)G(x) = t_i(x)s_i(x)G(x)$$

and finally

$$\beta(x)s_i(x) = t_i(x)s_i(x).$$

Now from Lemma 1 it is known that $\text{g.c.d.}(s_i(x), t_i(x)) = 1$ which implies that

$$s_i(x) = \lambda(x)s_i(x)$$

$$\beta(x) = \lambda(x)r_i(x) \text{ for some } \lambda(x).$$

Substituting into the original pair of equations (1) we have

$$s_i(x)G(x) + t_i(x)R(x) = r_i(x)$$

$$\lambda(x)s_i(x)G(x) + \lambda(x)t_i(x)R(x) = \alpha(x).$$

Multiplying the top equation by $\lambda(x)$ and comparing it may be seen

$$\alpha(x) = \lambda(x)r_i(x).$$

Thus, it may be finally shown that

$$\beta(x) = \lambda(x)r_i(x)$$

$$\alpha(x) = \lambda(x)r_i(x) \text{ for some } \lambda(x).$$

Recall that $\sigma(x)$ is the Goppa code error locator polynomial, and

$$\begin{aligned}\sigma(x) &= \alpha^2(x) + x\beta^2(x) \\ &= \lambda^2(x)\{r_i^2(x) + x t_i^2(x)\}\end{aligned}$$

after substitution.

But, by its construction, $\sigma(x)$ has only simple zeros. Thus $\lambda(x)$ is a constant, which may be taken to be 1 for ease of computation. Q.E.D.

In summary, to decode, one performs the following steps:

1. Compute the syndrome, $S(x)$.
2. Compute $T(x)$ such that $T(x)S(x) \equiv 1 \bmod G(x)$.
if $T(x) = x$, we are finished.
if $T(x) \neq x$, continue.
3. Compute $R(x)$ such that $R^2(x) \equiv T(x) + x \bmod G(x)$.
4. Solve $\beta(x)R(x) \equiv \sigma(x) \bmod G(x)$ using Euclid's algorithm. Stop when

$$\deg r_i(x) \leq s/2$$

$$\deg r_{i-1}(x) \leq s/2 + 1$$

and set

$$\alpha(x) = r_1(x)$$

$$\beta(x) = r_2(x).$$

Find the roots of

$$\sigma(x) = \sigma^2(x) + x \beta^2(x).$$

EXAMPLE 1

In order to give a concrete demonstration of the encryption and decryption processes, consider the following example.

Let $G(x) = x^2 + x + 1$ be the irreducible Goppa polynomial over $GF(2^3)$, where the ordering of the field elements is given by

$$0, \sigma^0, \sigma^1, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6$$

and σ is a root of the primitive polynomial $x^3 + x + 1$. The Goppa code defined by these conditions has $n=8$, $t=2$ and $k=2$. There are only four code words.

It can be shown that a generator matrix for this code is given by

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Next, this matrix is scrambled by forming $G' = SGP$, where S is nonsingular and P is a permutation matrix.

The following matrices are:

$$S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } P = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Then it is seen that

$$G' = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

From among the four possible message 2-tuples, choose $m = (10)$ and form the code word

$$mG' = (10110011) = v.$$

Since the code is capable of correcting up to 2 errors, select an error vector of weight 2. Let

$$e = (10010000) \text{ and form the cryptogram } r = v + e = (10110011) + (10010000) = (00100011).$$

Suppose that r is now transmitted through a channel and that no additional channel errors are inserted. At the receiving end, one begins the decrypting process by applying p^{-1} .

Form $rP^{-1} = (10010100)$, and then begin the Goppa decoding procedure.

Then form the syndrome

$$S(x) =$$

$$5 \quad \frac{1}{x+0} + \frac{1}{x+\alpha^2} + \frac{1}{x+\alpha^4} = \alpha^6 x + \alpha^5 \text{ mod } x^2 + x + 1.$$

Find $T(x)$ such that

$$10 \quad T(x)S(x) = 1 \text{ mod } x^2 + x + 1.$$

It can be seen that

$$T(x) = \alpha^2 x + \alpha^0 = \alpha^2 x + 1.$$

Next, find $R(x)$ such that

$$R^2(x) = T(x) + x = \alpha^2 x + 1 \text{ mod } x^2 + x + 1.$$

It can be seen that

$$R(x) = \alpha^2 x + \alpha^6.$$

Next, solve for $\alpha(x)$ and $\beta(x)$ in the congruence relation

$$25 \quad \beta(x)(\alpha^2 x + \alpha^6) = \alpha(x) \text{ mod } x^2 + x + 1.$$

Which finds that

$$30 \quad \alpha(x) = \alpha^2 x + \alpha^6 \\ \beta(x) = 1$$

and thus

$$35 \quad \sigma(x) = \alpha^2(x) + x\beta^2(x) \\ = \alpha^4 x^2 + x + \alpha^5.$$

The roots of $\sigma(x)$ are seen to be:

$$40 \quad x = \alpha^0$$

$$x = \alpha^1$$

Thus

45

$$mSG = (10010100) + (01100000) \\ = (11110100)$$

50 which is the corrected codeword.

But then it is straightforward to verify that

$$mS = (10)$$

55 and thus,

$$m = mS^{-1} = (10),$$

the original message vector.

60 A natural by-product of the decoding process is the permuted error vector

$$e' = (01100000).$$

The original error vector may be obtained by forming the product

$$eP = e = (10010000).$$

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 5,054,066

Page 1 of 2

DATED : October 1, 1991

INVENTOR(S) : Justus Riek, et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 2, line 14: delete "O"

Column 3, line 63: " $E_k(X)=Y$ " should read as

-- $E_k(X)=Y$ --

Column 3, line 65: " $D_k(Y)=X$ " should read as

-- $D_k(Y)=X$ --

Column 5, line 44: "differ" should read as

--differ.--

Column 7, line 40: " $e=e$ " should read as

-- $e' = e$ --

Column 9, line 30: Coeff_{13} should read as

--Coeff--

STAM0041728

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 5,054,066

Page 2 of 2

DATED : October 1, 1991

INVENTOR(S) : Justus Riek, et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 14, line 58: "weight =" should read as
--weight \leq --

Column 18, line 40: "Lenna" should read as
--Lenna--

Column 20, line 65: "s/2" should read as
-- $\lfloor s/2 \rfloor$ --

Column 20, line 67: "s/2" should read as
-- $\lfloor s/2 \rfloor$ --

Column 22, line 26: " + x03 1." should read as
-- + x + 1.--

Signed and Sealed this

Fourth Day of January, 1994

Attest:



BRUCE LEHMAN

Attesting Officer

Commissioner of Patents and Trademarks

STAM0041729

PATENT NUMBER		ORIGINAL CLASSIFICATION		CLASS		SUBCLASS		CROSS REFERENCE(S)	
		340		23		45			
PUBLICATION SERIAL NUMBER		CLASS		SUBCLASS		CROSS REFERENCE(S)			
08/672 116		340		23		45			
APPLICANT'S NAME (PLEASE PRINT)		CLASS		SUBCLASS		CROSS REFERENCE(S)			
Hambler		340		23		45			
P REISSUE, ORIGINAL PATENT NUMBER		CLASS		SUBCLASS		CROSS REFERENCE(S)			
		340		23		45			
INTERNATIONAL CLASSIFICATION		CLASS		SUBCLASS		CROSS REFERENCE(S)			
H04B		340		23		45			
1/00		340		23		45			
GROUP ART UNIT		CLASS		SUBCLASS		CROSS REFERENCE(S)			
2735		340		23		45			
ASSISTANT EXAMINER (PLEASE STAMP OR PRINT FULL NAME)		CLASS		SUBCLASS		CROSS REFERENCE(S)			
ORIAN GIMMELMAN		340		23		45			
PRIMARY EXAMINER (PLEASE STAMP OR PRINT FULL NAME)		CLASS		SUBCLASS		CROSS REFERENCE(S)			
		340		23		45			

ISSUE CLASSIFICATION SLIP

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

PTO 270
(REV. 5-91)

PATENT APPLICATION FEE DETERMINATION RECORD						Application or Docket Number <i>08/446,639</i>	
Effective October 1, 1994							
CLAIMS AS FILED - PART I							
(Column 1)		(Column 2)		(Column 3)		(Column 4)	
FOR	NUMBER FILED	NUMBER EXTRA					
BASIC FEE							
TOTAL CLAIMS	/	minus 20 =					
INDEPENDENT CLAIMS	/	minus 3 =					
MULTIPLE DEPENDENT CLAIM PRESENT							
* If the difference in column 1 is less than zero, enter "0" in column 2							
CLAIMS AS AMENDED - PART II							
(Column 1)		(Column 2)		(Column 3)		(Column 4)	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA				
Total	* 15	Minus	** 20	=	0		
Independent	* 4	Minus	*** 3	=	1		
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM							
(Column 1)		(Column 2)		(Column 3)		(Column 4)	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA				
Total	35	Minus	20	=	15		
Independent	10	Minus	4	=	6		
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM							
(Column 1)		(Column 2)		(Column 3)		(Column 4)	
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA				
Total	*	Minus	**	=			
Independent	*	Minus	***	=			
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM							
* 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.							

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
x\$11=	365.00	OR	x\$22=	730.00
x38=	—	OR	x76=	—
+120=	—	OR	+240=	—
TOTAL <i>365.00</i>		OR	TOTAL	

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
x\$11=	—	OR	x\$22=	—
x38=	38	OR	x76=	—
+120=	—	OR	+240=	—
TOTAL ADDIT. FEE <i>38</i>		OR	TOTAL ADDIT. FEE	

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
x\$11=	165.00	OR	x\$22=	—
x38=	38.00	OR	x76=	—
+120=	—	OR	+240=	—
TOTAL ADDIT. FEE <i>203.00</i>		OR	TOTAL ADDIT. FEE	

PACE DATA ENTRY CODING SHEET

U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office

1ST EXAMINER	DATE
2ND EXAMINER	DATE

APPLICATION NUMBER	TYPE APPL	FILING DATE	SPECIAL HANDLING	GROUP ART UNIT	CLASS	SHEETS OF DRAWING
146369	1	05/22/95	2	22-02	380	115

TOTAL CLAIMS	INDEPENDENT CLAIMS	SMALL ENTITY?	FILING FEE	FOREIGN LICENSE	ATTORNEY DOCKET NUMBER
1	1	1	1303	Y	6077-1143

CONTINUITY DATA

CONT STATUS CODE	PARENT APPLICATION SERIAL NUMBER	PCT APPLICATION SERIAL NUMBER	PARENT PATENT NUMBER	PARENT FILING DATE		
				MONTH	DAY	YEAR
1	22-02-1	1	5267314	09	14	93
1	22-02-2	1		1	1	92

PCT/FOREIGN APPLICATION DATA

FOREIGN PRIORITY CLAIMED	COUNTRY CODE	PCT/FOREIGN APPLICATION SERIAL NUMBER	FOREIGN FILING DATE

[illegible][illegible][illegible]

NAME SUFFIX					
STATE/CITY CODE					

[illegible]

NAME SUFFIX					
STATE/CTRY CODE					

1

TITLE OF INVENTION

PATENT APPLICATION FEE DETERMINATION RECORD					Application or Docket Number	
Effective October 1, 1996					8/872116	
CLAIMS AS FILED - PART I						
		(Column 1)	(Column 2)			
FOR	NUMBER FILED	NUMBER EXTRA				
BASIC FEE						
TOTAL CLAIMS		35 minus 20 = 15				
INDEPENDENT CLAIMS		10 minus 3 = 7				
MULTIPLE DEPENDENT CLAIM PRESENT						
<small>* If the difference in column 1 is less than zero, enter "0" in column 2</small>						
CLAIMS AS AMENDED - PART II						
		(Column 1)	(Column 2)	(Column 3)		
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			
	Total	13	35	= 8		
	Independent	12	10	= 2		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					
		(Column 1)	(Column 2)	(Column 3)		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			
	Total	54	43	= 11		
	Independent	12	12	=		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					
		(Column 1)	(Column 2)	(Column 3)		
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			
	Total	*	**	=		
	Independent	*	***	=		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					
<small>* 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.</small>						

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
	385.00	OR		770.00
x\$11=	165	OR	x\$22=	
x40=	280	OR	x80=	
+130=		OR	+260=	
TOTAL	830	OR	TOTAL	

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
x\$11=	88.00	OR	x\$22=	176
x40=	10.10	OR	x80=	
+130=		OR	+260=	
TOTAL ADDIT. FEE	98.10	OR	TOTAL ADDIT. FEE	

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
x\$11=	12.00	OR	x\$22=	
x40=		OR	x80=	
+130=		OR	+260=	
TOTAL ADDIT. FEE	12.00	OR	TOTAL ADDIT. FEE	

A full-page view of a blank sheet of graph paper. The grid consists of small squares formed by thin black lines. There are approximately 20 columns and 30 rows of squares. The paper has a slightly off-white or aged appearance.

[illegible][illegible][illegible][illegible]

U.S. Government Printing Office: 1996 - 404-474/40903

Staple Issue Slip Here

POSITION	ID NO.	DATE
CLASSIFIER	48	6/12/95
EXAMINER	105	7/18/95
TYPIST	116	7/10/95
VERIFIER	LAU	7-10-95
CORPS CORR.		
SPEC. HAND		
FILE MAINT.		
DRAFTING		

INDEX OF CLAIMS

Claim	Date
Final	Original
1	6/12/95
2	6/12/95
3	6/12/95
4	6/12/95
5	6/12/95
6	6/12/95
7	6/12/95
8	6/12/95
9	6/12/95
10	6/12/95
11	6/12/95
12	6/12/95
13	6/12/95
14	6/12/95
15	6/12/95
16	6/12/95
17	6/12/95
18	6/12/95
19	6/12/95
20	6/12/95
21	6/12/95
22	6/12/95
23	6/12/95
24	6/12/95
25	6/12/95
26	6/12/95
27	6/12/95
28	6/12/95
29	6/12/95
30	6/12/95
31	6/12/95
32	6/12/95
33	6/12/95
34	6/12/95
35	6/12/95
36	6/12/95
37	6/12/95
38	6/12/95
39	6/12/95
40	6/12/95
41	6/12/95
42	6/12/95
43	6/12/95
44	6/12/95
45	6/12/95
46	6/12/95
47	6/12/95
48	6/12/95
49	6/12/95
50	6/12/95
51	6/12/95
52	6/12/95
53	6/12/95
54	6/12/95
55	6/12/95
56	6/12/95
57	6/12/95
58	6/12/95
59	6/12/95
60	6/12/95
61	6/12/95
62	6/12/95
63	6/12/95
64	6/12/95
65	6/12/95
66	6/12/95
67	6/12/95
68	6/12/95
69	6/12/95
70	6/12/95
71	6/12/95
72	6/12/95
73	6/12/95
74	6/12/95
75	6/12/95
76	6/12/95
77	6/12/95
78	6/12/95
79	6/12/95
80	6/12/95
81	6/12/95
82	6/12/95
83	6/12/95
84	6/12/95
85	6/12/95
86	6/12/95
87	6/12/95
88	6/12/95
89	6/12/95
90	6/12/95
91	6/12/95
92	6/12/95
93	6/12/95
94	6/12/95
95	6/12/95
96	6/12/95
97	6/12/95
98	6/12/95
99	6/12/95
100	6/12/95

Claim	Date
Final	Original
1	6/12/95
2	6/12/95
3	6/12/95
4	6/12/95
5	6/12/95
6	6/12/95
7	6/12/95
8	6/12/95
9	6/12/95
10	6/12/95
11	6/12/95
12	6/12/95
13	6/12/95
14	6/12/95
15	6/12/95
16	6/12/95
17	6/12/95
18	6/12/95
19	6/12/95
20	6/12/95
21	6/12/95
22	6/12/95
23	6/12/95
24	6/12/95
25	6/12/95
26	6/12/95
27	6/12/95
28	6/12/95
29	6/12/95
30	6/12/95
31	6/12/95
32	6/12/95
33	6/12/95
34	6/12/95
35	6/12/95
36	6/12/95
37	6/12/95
38	6/12/95
39	6/12/95
40	6/12/95
41	6/12/95
42	6/12/95
43	6/12/95
44	6/12/95
45	6/12/95
46	6/12/95
47	6/12/95
48	6/12/95
49	6/12/95
50	6/12/95
51	6/12/95
52	6/12/95
53	6/12/95
54	6/12/95
55	6/12/95
56	6/12/95
57	6/12/95
58	6/12/95
59	6/12/95
60	6/12/95
61	6/12/95
62	6/12/95
63	6/12/95
64	6/12/95
65	6/12/95
66	6/12/95
67	6/12/95
68	6/12/95
69	6/12/95
70	6/12/95
71	6/12/95
72	6/12/95
73	6/12/95
74	6/12/95
75	6/12/95
76	6/12/95
77	6/12/95
78	6/12/95
79	6/12/95
80	6/12/95
81	6/12/95
82	6/12/95
83	6/12/95
84	6/12/95
85	6/12/95
86	6/12/95
87	6/12/95
88	6/12/95
89	6/12/95
90	6/12/95
91	6/12/95
92	6/12/95
93	6/12/95
94	6/12/95
95	6/12/95
96	6/12/95
97	6/12/95
98	6/12/95
99	6/12/95
100	6/12/95

SYMBOLS
 ✓ Rejected
 * Allowed
 (Through numbers) Canceled
 N Restricted
 NI Non-elected
 I Interference
 A Appeal
 O Objected

TITLE OF INVENTION

STAM0041737

SEARCHED			
Class	Sub.	Date	Exmr.
340	825.30 825.31 825.33 825.34	12/8/45	BZ
380	23 24 25 43 45 4		
	update search	6/18/46	BZ
	update search	3/24/47	BZ

INTERFERENCE SEARCHED			
Class	Sub.	Date	Exmr.
Search	None	3/24/47	BZ

SEARCH NOTES		
	Date	Exmr.
<p>Out of line -10440 N. 10440 None</p>	3/24/47	BZ

STAM0041738

Staple Issue Slip Here

06/872, 116

POSITION	ID NO.	DATE
CLASSIFIER		
EXAMINER	410	3/8/97
TYPIST		
VERIFIER		
CORPS CORR.		
SPEC. HAND		
FILE MAINT.		
DRAFTING		

INDEX OF CLAIMS

Claim	Date
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	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	

Claim	Date
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	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	
52	
53	
54	
55	
56	
57	
58	
59	
60	
61	
62	
63	
64	
65	
66	
67	
68	
69	
70	
71	
72	
73	
74	
75	
76	
77	
78	
79	
80	
81	
82	
83	
84	
85	
86	
87	
88	
89	
90	
91	
92	
93	
94	
95	
96	
97	
98	
99	
100	

SYMBOLS
 ✓ Rejected
 = Allowed
 - (Through numbers) Canceled
 * Restricted
 N Non-elected
 I Interference
 A Appeal
 O Objected

STAM0041739

SEARCHED			
Class	Sub.	Date	Exmr.
340	340 825.30 .31 .33 .34	4/6/93	BT
380	23 24 25 4 43 45		
235	382 update search	2/24/99	BT

INTERFERENCE SEARCHED			
Class	Sub.	Date	Exmr.
search	above	2/24/99	BT

SEARCH NOTES		
	Date	Exmr.
update search none	2/24/99	BT

08/872, 116

W/446369

PATENT APPLICATION



08446369

APPROVED FOR LICENSE

JUN 1 1995
INITIALS 149529

Date
Entered
or
Counted

CONTENTS

Date
Received
or
Mailed

1.	Application	papers.	
2.	Patent 11/2/91		5-22-91
3.	Patent 11/2/91		5-22-91
4.	Rej 3 months		12-11-95
5.	Rej 3 months		12-11-95
6.	Rej 3 months		12-11-95
7.	Rej 3 months		12-11-95
8.	Rej 3 months		12-11-95
9.	Rej 3 months		12-11-95
10.	Rej 3 months		12-11-95
11.	Rej 3 months		12-11-95
12.	Rej 3 months		12-11-95
13.	Rej 3 months		12-11-95
14.	Rej 3 months		12-11-95
15.	Rej 3 months		12-11-95
16.	Rej 3 months		12-11-95
17.	Rej 3 months		12-11-95
18.	Rej 3 months		12-11-95
19.	Rej 3 months		12-11-95
20.	Rej 3 months		12-11-95
21.	Rej 3 months		12-11-95
22.	Rej 3 months		12-11-95
23.	Rej 3 months		12-11-95
24.	Rej 3 months		12-11-95
25.	Rej 3 months		12-11-95
26.	Rej 3 months		12-11-95
27.	Rej 3 months		12-11-95
28.	Rej 3 months		12-11-95
29.	Rej 3 months		12-11-95
30.	Rej 3 months		12-11-95
31.	Rej 3 months		12-11-95
32.	Rej 3 months		12-11-95

(FRONT)

STAM0041741

U.S. PRO.
08/872116
06/10/97

PATENT APPLICATION

APPROVED FOR LICENSE ☐

INITIALS _____



08872116

CONTENTS

Date
Entered
or
Counted

Date
Received
or
Mailed

1.	Application	papers.
22	Corrected claim receipt	09-29-97
23	Declaration	June 18/1997
24	Receipt	June 18/1997
25	Receipt	June 18/1997
26	Receipt	June 18/1997
27	Receipt	June 18/1997
28	Receipt	June 18/1997
29	Receipt	June 18/1997
30	Receipt	June 18/1997
31	Receipt	June 18/1997
32	Receipt	June 18/1997
33	Receipt	June 18/1997
34	Receipt	June 18/1997
35	Receipt	June 18/1997
36	Receipt	June 18/1997
37	Receipt	June 18/1997
38	Receipt	June 18/1997
39	Receipt	June 18/1997
40	Receipt	June 18/1997
41	Receipt	June 18/1997
42	Receipt	June 18/1997
43	Receipt	June 18/1997
44	Receipt	June 18/1997
45	Receipt	June 18/1997
46	Receipt	June 18/1997
47	Receipt	June 18/1997
48	Receipt	June 18/1997
49	Receipt	June 18/1997
50	Receipt	June 18/1997
51	Receipt	June 18/1997
52	Receipt	June 18/1997
53	Receipt	June 18/1997
54	Receipt	June 18/1997
55	Receipt	June 18/1997
56	Receipt	June 18/1997
57	Receipt	June 18/1997
58	Receipt	June 18/1997
59	Receipt	June 18/1997
60	Receipt	June 18/1997
61	Receipt	June 18/1997
62	Receipt	June 18/1997
63	Receipt	June 18/1997
64	Receipt	June 18/1997
65	Receipt	June 18/1997
66	Receipt	June 18/1997
67	Receipt	June 18/1997
68	Receipt	June 18/1997
69	Receipt	June 18/1997
70	Receipt	June 18/1997
71	Receipt	June 18/1997
72	Receipt	June 18/1997
73	Receipt	June 18/1997
74	Receipt	June 18/1997
75	Receipt	June 18/1997
76	Receipt	June 18/1997
77	Receipt	June 18/1997
78	Receipt	June 18/1997
79	Receipt	June 18/1997
80	Receipt	June 18/1997
81	Receipt	June 18/1997
82	Receipt	June 18/1997
83	Receipt	June 18/1997
84	Receipt	June 18/1997
85	Receipt	June 18/1997
86	Receipt	June 18/1997
87	Receipt	June 18/1997
88	Receipt	June 18/1997
89	Receipt	June 18/1997
90	Receipt	June 18/1997
91	Receipt	June 18/1997
92	Receipt	June 18/1997
93	Receipt	June 18/1997
94	Receipt	June 18/1997
95	Receipt	June 18/1997
96	Receipt	June 18/1997
97	Receipt	June 18/1997
98	Receipt	June 18/1997
99	Receipt	June 18/1997
100	Receipt	June 18/1997

(FRONT)

STAM0041742

A COVERBINDER COVER 1-800-366-6062
1 1/4" Classic PTO 16839 for 291 to 300 sheets



STAM0041743



PTO-1683
(Rev. 7-96)

STAM0041744