PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G07F 7/10

A1

(11) International Publication Number: WO 98/36386

(43) International Publication Date: 20 August 1998 (20.08.98)

(21) International Application Number: PCT/EP97/00688

(22) International Filing Date: 13 February 1997 (13.02.97)

(71) Applicant: KONINKLIJKE PTT NEDERLAND N.V. [NL/NL]; Stationsplein 7, NL-9726 AE Groningen (NL).

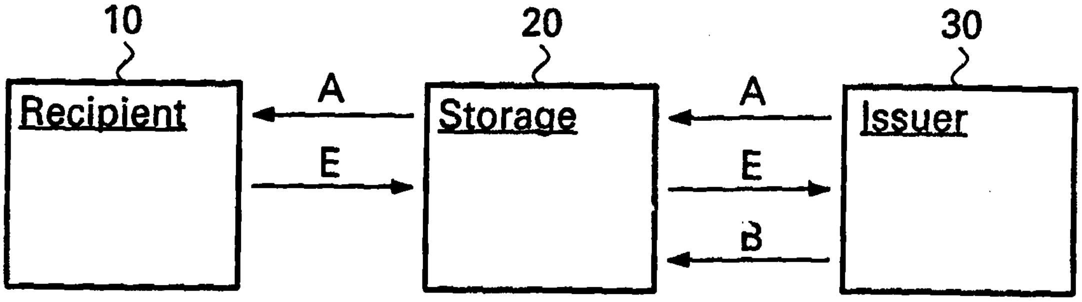
(72) Inventors: DE ROOIJ, Peter, Jacobus, Nicolaas; Wijnpersstraat 30/13, B-3000 Leuven (BE). BOSSELAERS, Antoon, Wilfried, Jan; Naamsestraat 149, B-3000 Leuven (BE).

(74) Agent: BEITSMA, Gerhard, Romano; Koninklijke PTT Nederland N.V., P.O. Box 95321, NL-2509 CH The Hague (NL).

(81) Designated States: AU, CA, CN, CZ, EE, HU, IL, JP, KR, LT, LV, MX, NO, NZ, PL, SG, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: METHOD OF SECURELY STORING AND RETRIEVING MONETARY DATA



(57) Abstract

A method of securely storing and retrieving monetary values, such as electronic cheques and electronic coins, is disclosed. In an interactive protocol between an issuer (e.g. a bank terminal) and a recipient (e.g. a smart card) of electronic money, authentication values (A, B, ...) are produced and are stored in an external storage (e.g. an electronic wallet). At a later stage, the protocol is repeated between the recipient and the storage to securely retrieve the stored authentication values.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

Method of securely storing and retrieving monetary data.

BACKGROUND OF THE INVENTION

The present invention relates to the storing and retrieving of monetary data. More specifically, the present invention relates to the storing of monetary data, such as data identifying electronic cheques and electronic coins, in a storage medium, and to the later retrieval of the stored data by a means for electronic financial transactions, such as a so-called smart card.

Electronic cheques and coins necessarily take up a fair amount of memory space, as they comprise various authentication data, such as a signature from a bank (issuer). As the storage capacity of a smart card is usually limited, the need arises to externally store data which ensure the validity of electronic money. However, it must be assured that the data retrieved from storage can be trusted, i.e. are valid data. To this end it is possible to arrange for an on-line protocol with the issuer each time data are loaded from storage. This is however time-consuming and often involves communications costs.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a method for safely storing and retrieving data, such as monetary data, in which the retrieval of data may be executed off-line. It is a further object of the present invention to provide a method which is independent of the specific type of data, such as electronic cheques or coins. It is a still further object of the invention to provide a method in which the validity of monetary data may be derived from an interactive protocol.

To this end, the present invention provides a method of securely storing and retrieving data, the method comprising a first phase comprising an interaction between an issuer and a recipient, data comprising authentication values being stored in the recipient and in a storage, and a second phase comprising an interaction between the storage and the recipient, data being retrieved from the storage and being verified by means of the authentication values and at least one authentication value stored in the recipient.

By substantially repeating in the second phase the interaction of the first phase, a secure protocol may be achieved. The secure protocol effectively eliminates the possibility of loading incorrect monetary data, such as used or forged electronic cheques, into the recipient.

Preferably, a first authentication value comprises a commitment produced by the issuer. Such a commitment, for example comprising an electronic signature, allows valid electronic money to be used.

Advantageously, in the second phase the storage verifies the authentication value received from the recipient.

The method of the present invention thus allows the validity of (monetary) data to be derived from an interactive protocol between an issuer and a recipient, but does not require an interaction with the issuer while retrieving stored data.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows schematically an IC card and an electronic wallet for interacting with the IC card.

Fig. 2 shows schematically a system for electronic payments, as well as the exchange of data according to a first phase of the method of the present invention.

Fig. 3 shows schematically a system for electronic payments, as well as the exchange of data according to a second phase of the method of the present invention.

Fig. 4 shows schematically a first phase of the method according to the present invention.

Fig. 5 shows schematically a second phase of the method according to the present invention.

EXEMPLARY EMBODIMENTS

The so-called electronic wallet 2 shown in Fig. 1 is a device for interacting with an IC card 1. The wallet has a keyboard 5, a slot 4 for inserting the card 1, means for communicating with the inserted card via the card contacts 3, and means for communicating with an external terminal, such as a cash register (not shown). Such a terminal may comprise a card reader and/or an infra-red card interface for communicating with the card, preferably via the wallet. The terminal may further comprise means for establishing an on-line connection with a money issuing institution, such as a bank, and/or a secure module for securely storing monetary values or the like.

The wallet 2 allows a user to interact with the card 1 via a keyboard 5 and a display 6. The wallet 2 allows the user to e.g. check balances, transfer balances between accounts, authorize payments, and the like. The wallet also provides a storage for storing electronic cheques, coins and the like, and thus acts as a storage extension for the card. The card 1 is provided with an integrated circuit (IC) arranged under the contacts 3. The integrated circuit may comprise a processor, a memory and I/O (input/output) means. As the memory size of present day smart cards is limited, a wallet may advantageously be used to store for later retrieval payment data which cannot be stored on the card.

The system shown schematically and by way of example in Fig. 2 comprises a recipient 10, a storage 20 and an issuer 30. The recipient 10 and the storage 20 may correspond with the card 1 and the wallet 2 of Fig. 1 respectively. The issuer 30, which may be a bank or another monetary data providing institution, comprises a terminal suitable for interaction with the storage (wallet) 20.

In the following text, it will be assumed that the issuer (e.g. bank terminal) 30 issues electronic money, such as electronic cheques and coins represented by suitable data, while the recipient (e.g. smart card) 10 receives the electronic money. The storage (wallet) 20 is used both as an intermediary between the issuer 30 and the recipient 10 and as a storage proper for electronic money not stored on the card. It will be understood that the word "money" in this text is meant to comprise various representations of monetary and other values, and specifically comprises electronic cheques and coins. In the following, the terms "monetary data" or just "data" will be used to indicate data related to "money", and especially data representing electronic cheques and coins. However, the method of the present invention may also be applied to other data, such as confidential data.

In the method of the invention, the issuer 30 and the recipient 10 exchange messages as indicated in Fig. 2. In summary, the recipient generates an identification value, performs an interactive protocol with the issuer while storing the relevant data in the storage, and discards most of the data while keeping sufficient data to regenerate the identification value. When retrieving the data, the identification value is regenerated, the interactive protocol is performed with the storage 20 rather than with the issuer 30 as indicated in Fig. 3, and the relevant data are stored in the recipient 10. The identification value and the initial value (seed) for regenerating the identification value may then be discarded. It will be understood that instead of a value for regenerating the identification value, the identification value itself may be temporarily stored.

In the following, it will be assumed that the data exchange between the issuer 30 and the recipient 10 takes place via the storage 20, i.e all data pass through the storage 20. It will be understood that it is just as well possible for the issuer 30 and the recipient 10 to communicate directly and to copy the relevant exchanged data to the storage 20.

Reference will now be made to Fig. 4 in conjunction with Fig. 3. It is noted that in Figs. 4 and 5 the recipient, storage and issuer are denoted by R, S and I respectively. In the method as depicted in Fig. 4, the generation of monetary data (such as electronic cheques) is initiated in step 100, for instance by the recipient 10 sending a relevant request to the issuer 30. In step 101, the issuer (I) generates a commitment A associated with one or more groups of monetary data (electronic cheques and/or coins). This commitment A may be produced by generating and using a suitable cryptographic function F_1 operating upon a random value W: $A = F_1(W)$. An example of a suitable function F_1 is discrete exponentiation modulo p with generator g of the order q, where q divides p-1 and where p and q are predetermined (prime) numbers: $A = F_1(W) = g^W \bmod p$. The random value W may be predetermined or may be produced in step 101 using a random number generator.

The commitment A, by means of which the issuer commits himself to the monetary data, is sent to the recipient (R), in the present example via the storage (S) which stores the commitment A. The commitment A may be (temporarily) stored in the recipient as well.

In step 102, upon receiving the commitment A, the recipient generates an identification value C. This is for example a random number, generated on the basis of a seed X using a second (random) function F_2: $C = F_2(X)$. Optionally, the seed X is the result of combining a (fixed) base seed X_0 and an index Y. The index Y, which may have a considerably shorter length than the seed X, may e.g. indicate an entry in a table of seeds. Preferably, the index Y indicates how many times the function F_2 is to be applied, starting from the base seed X_0, to obtain the desired seed X. For example, if Y is equal to 3, the seed X may be obtained by applying the (random) function F_2 three times: $X = F_2(F_2(F_2(X_0)))$.

The seed X is stored in the recipient (R). If a base seed X_0 is used, this base seed is preferably permanently stored in the recipient, while the index Y may be stored in the recipient (R) or the storage (S).

Instead of storing the seed X or the index Y, it is also possible to store the value C. In practice, C will comprise more bits than Y and will thus require more storage space, making the storing of Y more economical.

Preferably, the relevant value (C, X or X_0) is stored in such a way so as to be directly linkable to a value A. That is, the storage may comprise a plurality of values A (e.g. each corresponding with a cheque), a relevant value (C, X or X_0) being stored for each value A.

Subsequent to the computation of the identification value C, the recipient (R) generates a "fingerprint" E of the identification value C using a third function F_3: $E = F_3(C)$. Preferably, the fingerprint E also involves the value A: $E = F_3(C,A)$. The function F_3 may for example involve subjecting the combination of the identification value C and the commitment A to a so-called hash function H: $E = H(A,C)$. This fingerprint E, which identifies the identification value C but from which the value C cannot be derived, is sent to the issuer.

In step 103, the issuer (I) uses the received fingerprint E to produce a value B using a fourth function F_4 : $B = F_4(E)$. Such a function involves, for example, multiplying the fingerprint E by a secret key K_S modulo q and adding the result to the previously used random value W: $B = W + E.K_S \bmod q$. The value B thus derived is stored in the storage (S). The value B, which is the authenticating value of monetary data, may optionally be sent to the recipient (R), e.g. for verification purposes, but this is not essential.

It should be noted that the above scheme serves to produce data (e.g. cheques) to which both the issuer and the recipient have contributed. The final value B is derived by the issuer from the value E, which is in turn derived by the recipient from the value A. As the value A was produced by the issuer, the values concerned are mutually linked.

In a first embodiment of the present invention, the value B is not passed on to the recipient (R) but stored in the storage (S) for later retrieval. In a second embodiment of the present invention, the value B is not only stored in the storage (S), but also sent to the recipient (R) for verification purposes. In the second embodiment, an additional step 104 (not shown in Fig. 4) is carried out in which additional data D may be derived from the values A, B, C and the public key K_P associated with the secret key K_S. These data D, which are associated with the value B, provide additional information with respect to the monetary values concerned. The data D may further be verified using the same values, for example by verifying whether $F_5(A,B,E) = 0$, where $D = (A,B,E)$, i.e. the combination of A, B and E (or C). In actual implementations, it may be verified whether $g^B = A.K_P^E \bmod p$. The seed X, or alternatively the identification value C, is stored by the recipient R. Further data, including the data D and the values A, B and C (or E), may now be discarded, as the generation part of the method is completed.

Reference will now be made to Fig. 5 in conjunction with Fig. 3, in which figures the reconstruction phase is depicted. The reconstruction phase of the method of the present invention is initiated by the recipient (R) in step 110. In step 111 the commitment A is retrieved from the storage S. If an index Y was used in step 102 to determine the seed X, this index Y is also retrieved. It should be noted that the storage should not contain both Y and X_0, or X, as that would allow the storage to produce monetary data without the involvement of the recipient.

In step 112, the identification value C is regenerated on the basis of the seed X. The fingerprint E of the identification value C is also regenerated, for example by subjecting the combination of the identification value C and the commitment A to a so-called hash function: $E = H(A,C)$. This fingerprint E, which identifies the identification value C but from which the value C cannot be derived, is sent to the storage S.

In step 113, the stored value B is retrieved. Optionally, the fingerprint E can be checked by verifying whether $F_5(A,B,E) = 0$. In actual implementations, it may be verified whether $g^B = A.K_P^E \bmod p$. Subsequently, in step 114 the retrieved value B is used to regenerate the data D from A, B, C and the public key K_P of the issuer I. The validity of the thus regenerated data D may further be verified using the same values, for example by verifying $g^R = A.K_P^E \bmod p$.

In the above method, data (e.g. D) are generated on-line and regenerated off-line. The method thus offers the possibility of regenerating data (D) without the need to involve the issuer. The issuer only "signs" the data (in a challenge-signed response exchange involving E and B) in the first phase. The method uses a controlled replay of the first phase to regenerate data in the second phase, where the recipient verifies the data. With the aid of the keys K_S and K_P, a further protection of the data is achieved.

As the first (generation) phase may be considered to constitute an interrupted withdrawal of (e.g. monetary) data, which withdrawal is substantially repeated by the recipient in the second (reconstruction) phase, the recipient is capable of using identical protocols in both phases. As a result, there is no need for storing in the recipient additional code (software) for the second phase, thus effectively saving memory space.

In the above example, an electronic wallet has been shown as an example of an external storage. The invention may also be used with other types of storage, such as another card or other terminal.

It will be understood by those skilled in the art that the embodiments described above are given by way of example only and that many modifications and additions are possible without departing from the scope of the present invention.

CLAIMS

1. Method of securely storing and retrieving data, the method comprising a first phase comprising an interaction between an issuer and a recipient, data comprising authentication values (A, B) being stored in a storage, and a second phase comprising an interaction between the storage and the recipient, data being retrieved from the storage and being verified by means of the authentication values (e.g. A, B) and at least one authentication value (C) stored in the recipient.

2. Method according to claim 1, in which a first authentication value (A) comprises a commitment produced by the issuer.

3. Method according to claim 1 or 2, in which a second authentication value (E) comprises a fingerprint of the authentication value (C) stored in the recipient.

4. Method according to claim 3, in which instead of the authentication value (C) a value (X) from which the authentication value can be regenerated is stored in the recipient.

5. Method according to any of the preceding claims, in which the third authentication value (B) is produced by the issuer on the basis of the second authentication value (E) and secret data, such as a key.

6. Method according to any of the preceding claims, in which in the second phase the retrieved data (A, B, ...) are used to regenerate monetary data.

7. Method according to claim 6, in which the regenerated data are verified by means of the issuer's public key.

8. Method according to any of the preceding claims, in which the recipient is constituted by a smart card and the storage is constituted by an electronic wallet.

9. Electronic cheque, regenerated by means of the method according to any of the preceding claims.

10. System for electronic monetary transactions, arranged for storing and retrieving data according to any of the claims 1 through 9.

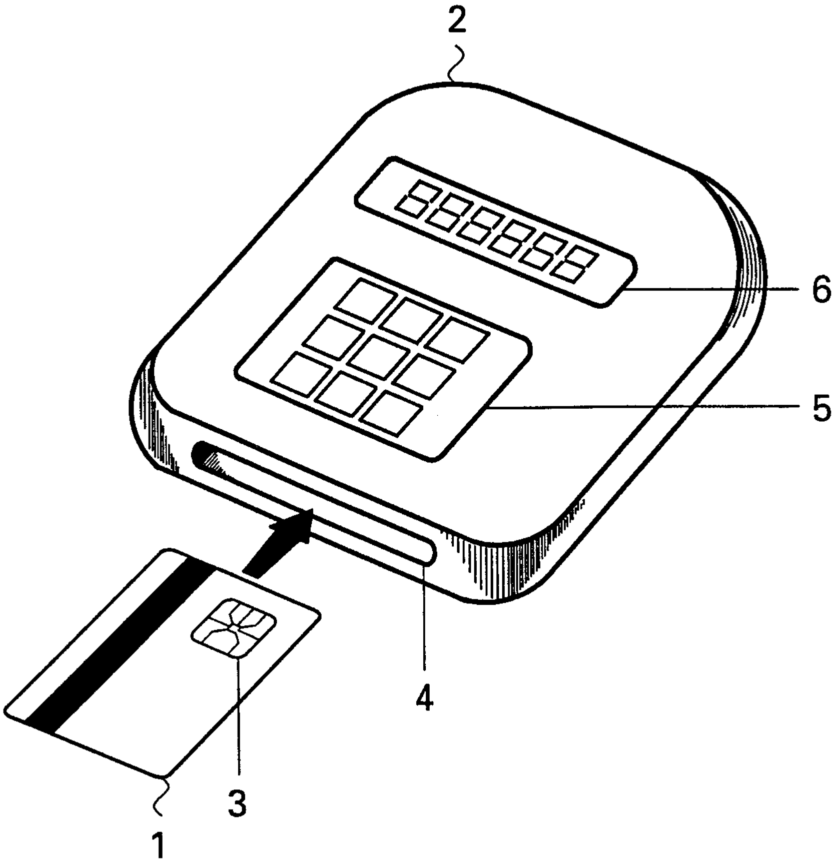


Fig. 1

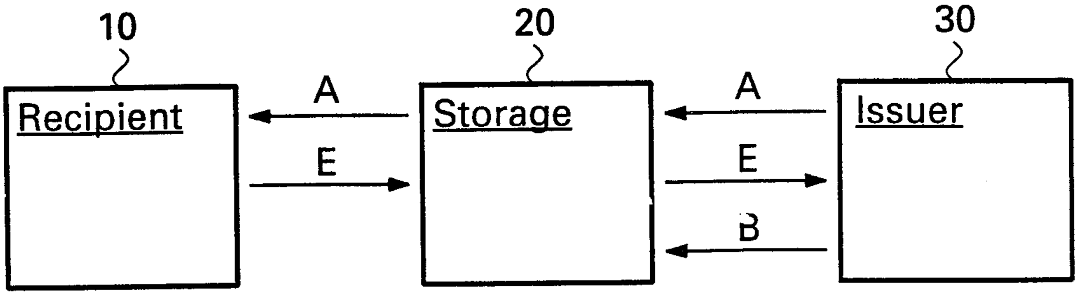

10
20
30
Recipient
Storage
Issuer
A
E
A
E
B

Fig. 2

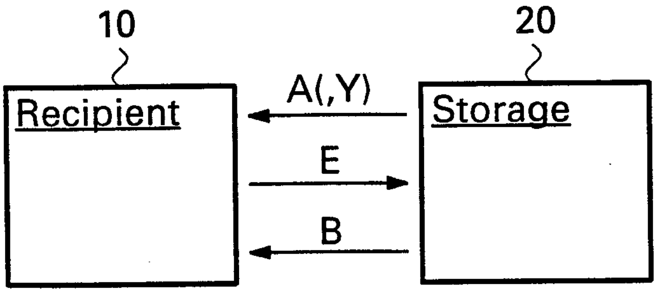

10
20
Recipient
Storage
A(,Y)
E
B

Fig. 3

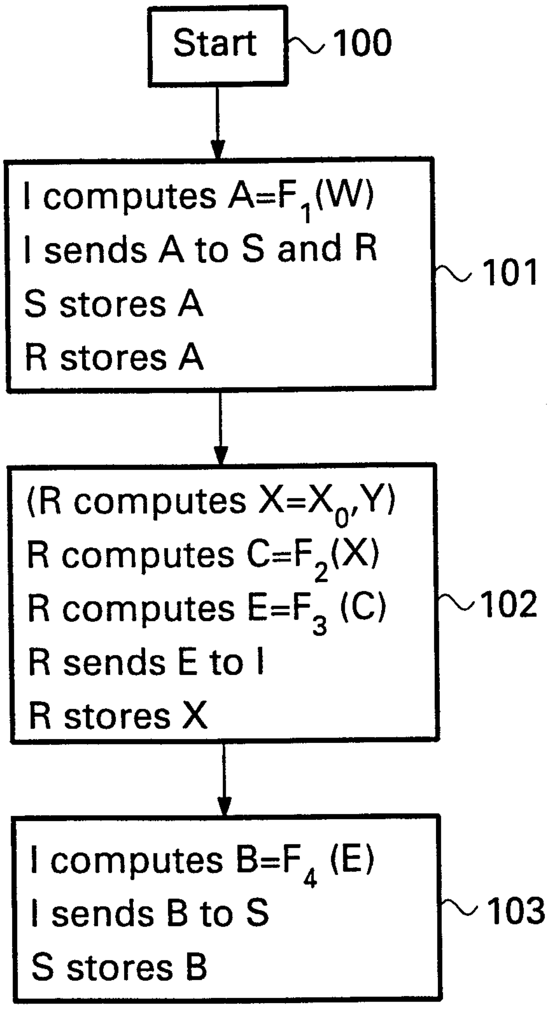

Start
100
I computes $A=F_1(W)$
I sends A to S and R
S stores A
R stores A
101
(R computes $X=X_0,Y$)
R computes $C=F_2(X)$
R computes $E=F_3$ (C)
R sends E to I
R stores X
102
I computes $B=F_4$ (E)
I sends B to S
S stores B
103

Fig. 4

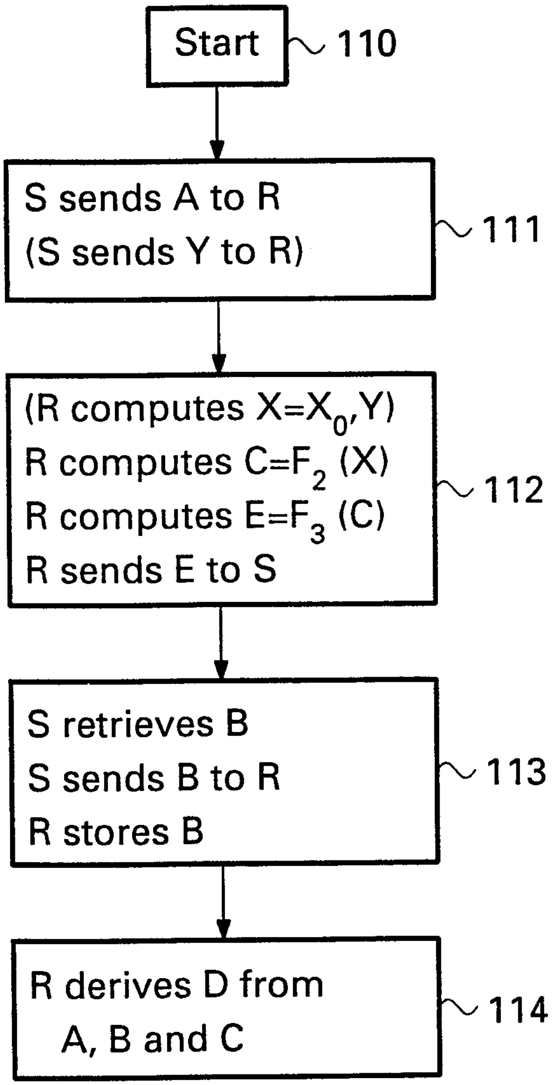

Start
110
S sends A to R
(S sends Y to R)
111
(R computes $X=X_0,Y$)
R computes $C=F_2$ (X)
R computes $E=F_3$ (C)
R sends E to S
112
S retrieves B
S sends B to R
R stores B
113
R derives D from A, B and C
114

Fig. 5

INTERNATIONAL SEARCH REPORT

Ir ational Application No
PCT/EP 97/00688

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 . G07F7/10

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 138 219 A (TOSHIBA) 24 April 1985 see abstract; claims; figures ---	1,3,6,7, 10
A	EP 0 546 584 A (MATSUSHITA ELECTRIC INDUSTRIAL) 16 June 1993 see abstract; claims; figures ---	1,6,8-10
A	WO 91 13411 A (M. VILLIKARI) 5 September 1991 ---	
A	EP 0 623 903 A (PITNEY BOWES) 9 November 1994 ---	
A	WO 91 10214 A (MIKROMAX INDUSTRITEKNIK) 11 July 1991 -----	

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

1

Date of the actual completion of the international search 29 May 1997	Date of mailing of the international search report 13.06.97
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Authorized officer David, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 97/00688

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0138219 A	24-04-85	JP 60084686 A	14-05-85
		DE 3473660 A	29-09-88
		US 4672182 A	09-06-87
EP 0546584 A	16-06-93	JP 6019945 A	28-01-94
		JP 6020106 A	28-01-94
		JP 8027815 B	21-03-96
WO 9113411 A	05-09-91	AU 7315691 A	18-09-91
		EP 0524186 A	27-01-93
EP 0623903 A	09-11-94	CA 2122843 A,C	07-11-94
WO 9110214 A	11-07-91	SE 464896 B	24-06-91
		AU 6978791 A	24-07-91
		SE 8904335 A	23-06-91