9606188-2
APX

This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

Method, sender apparatus and receiver apparatus for modulo operation

The present invention relates to a method, to a sender apparatus and to a receiver apparatus for modulo operation.

Background

In access control systems, e.g. pay TV systems, square, or more general, d-th roots modulo X are used where X is a composite number having at least two large prime factors. Typically the length of such a number X (denoted |X|) is 64 bytes.
If a sender, e.g. a smart-card, communicates with a receiver only few data are transmitted in order to save time. But this results in an increased number of computation operations in the sender and/or receiver.

Invention

It is one object of the invention to disclose a method for time-reduced modulo operations. This object is reached by the inventive method disclosed in claim 1.

In principle the inventive method consists in secure sending of a number S = D mod X or of a set of numbers S(j) = D(j) mod X, j = 1,...,i, from a sender device 28 to a receiver device 27, whereby X is a product of at least two big prime numbers and D is greater than X, comprising the following steps:
- picking a random number A or a set of random numbers A(j) by said sender device;
- calculating in said sender a value E = D+A*X or a set of values E(j) = D(j)+A(j)*X, whereby X is stored in said sender, or calculating in said sender a set of values E(j) =

THIS SHEET HAS BEEN REPLACED

D(j)*B, whereby a fixed number B = A*X is stored in said sender;
- transmitting via an interface 10 said value and said values, respectively, from said sender to said receiver;
- calculating by said receiver S = E mod X or S(j) = E(j) mod X, whereby the number X is stored in said receiver device.

Advantageous additional embodiments of the inventive method are resulting from the respective dependent claims.

It is a further object of the invention to disclose a sender apparatus which utilizes the inventive method. This object is reached by the inventive apparatus disclosed in claim 6.

In principle the inventive sender apparatus consists in first computation means 25, first memory means 26 which are connected to said first computation means and first data exchange means 24 which are connected to said first computation means, whereby either
said first memory means store said modulus X and said first computation means select said random number A or random numbers A(j) and calculate said value E = D+A*X or calculate said set of values E(j) = D(j)+A(j)*X
or
said first memory means store said fixed number B and said first computation means calculate said set of values E(j) = D(j)+B
and whereby said first data exchange means 24 send said value E or said set of values E(j) to said receiver device 27.

Advantageous additional embodiments of the inventive sender apparatus are resulting from the respective dependent claims.

It is a further object of the invention to disclose a receiver apparatus which utilizes the inventive method. This object is reached by the inventive apparatus disclosed in claim 7.

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

In principle the inventive receiver apparatus consists in second computation means 22, second memory means 21 which are connected to said second computation means and second data exchange means 23 which are connected to said second computation means, whereby said second memory means store said modulus X and said second computation means calculate the modulo function S = E mod X of said value E or calculate a set of modulo functions S(j) = E(j) mod X of said set of values E(j).

Advantageous additional embodiments of the inventive receiver apparatus are resulting from the respective dependent claims.

The invention is applicable when a first cryptographic device (sender) communicates with a second cryptographic device (receiver), especially when the devices use a modulo-based protocol. Thereby the required number of modular operations is reduced or even eliminated. It can be avoided to do modular operations by the first device.
This is particularly advantageous when said first device, e.g. a smart-card, has a weaker computional power (e.g. less RAM and/or ROM capacity, slower clock rate) than said second device (e.g. a powerful processor acting as a verifier).

There are such access control systems where all the numbers appearing in the first ("weaker") device have a size n*|X| bytes before modular reduction, where n is a very small integer, typically 2 or 3.
There are different variants of the inventive method.
First variant:
Let D be a number of length n*|X| bytes.
The sender wishes to communicate S = D mod X to the receiver. For avoiding the modular reduction the sender chooses a random number A, computes E = D+A*X and sends this value E to the receiver. Since A is random the value of D is hidden in E and the receiver can calculate S by:
S = E mod X, because

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

E mod X = D mod X + A*X mod X = D mod X.

Second variant:
The sender wishes to communicate a set of i numbers S(j) = D(j) mod X to the receiver.
Number A is a secret of the sender. The sender keeps in a ROM a pre-calculated constant B, B = A*X.
As before, let D(1),...,D(i) be a set of numbers (all bigger than X) such that the set of values S(j) is to be send to the receiver. Then these D(i) can be hidden by sending to the receiver E(1) = D(1)+B,...,E(i) = D(i)+B. The receiver will recover S(j) by calculating:
S(j) = E(j) mod X, because
E(j) mod X = D(j) mod X + B mod X = D(j) mod X.
Number i may have a value of 10.

The first and the second variant can be modified. This modification fits especially to smart-card applications. It allows the sender to perform squarings or a multiplication (which result is E) with only |X| RAM bytes.
For doing so the sender computes only the |X| lower bytes of E (denoted Low(E)) and sends them to the receiver. This computation of Low(E) requires only |X| RAM cells. After the receiver gets Low(E), the sender can reuse his |X| RAM bytes to compute the |X| higher bytes of E (denoted High(E)). When the receiver gets High(E) it calculates
E = Concatenation (High(E),Low(E))
and continues its calculations as before.

This Sheet Has Been Replaced



This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

Drawings

Preferred embodiments of the invention will now be described with reference to the accompanying drawings, in which:

Fig. 1 shows an inventive communication protocol between the sender and the receiver;
Fig. 2 shows a sender and a receiver.

Preferred embodiments

Fig. 1 shows an interface 10 between a sender, e.g. a weak processor in a smart-card, and a receiver, e.g. a pay TV decoder, which may contain a powerful processor for calculating the modulo function. The microprocessor in the sender prepares a first number D or a first set of numbers D(j). Then it chooses a random number A and calculates E = D+A*X or it adds value B to each number D(j) and sends E and the set E(j), respectively, via interface 10 to the receiver side. The receiver calculates S = E mod X or S(j) = E(j) mod X from the received numbers.
Advantageous the final length |E| or |E(j)| of E and E(j), respectively, is less than four times the length |X| of X.

In Fig. 2 a receiver device 27 and a sender device 28 are depicted. The sender device contains a first microprocessor 25, first memory means 26 which are connected to microprocessor 25 and a first connector 24 for data exchange with receiver device 27.
The receiver device 27 contains a second microprocessor 22, second memory means 21 which are connected to microprocessor 22 and a second connector 23 for data exchange with sender device 28.
First connector 24 and second connector 23 represent the interface 10 in Fig. 1. The first memory means 26 store intermediate calculation results and/or values X and/or B or

THIS SHEET HAS BEEN REPLACED

Low(E)/High(E). First microprocessor 25 computes data as shown in the left side of Fig. 1.
The second memory means 21 store value X and/or intermediate results. Second microprocessor 22 computes data as shown in the right side of Fig. 1.

The invention can be used for identification (VideoCrypt or EuroCrypt Pay TV system) and/or digital signature (credit cards) and/or encryption, especially together with one or more of the following systems for getting in the receiver modulo calculated results without respective modulo calculation in the sender:

- Fiat-Shamir;
- Feige-Fiat-Shamir;
- Quisquater-Guillou;
- Fischer-Micali-Rackoff;
- Naccache (EP-A-91400111, EP-A-91400301);
- RSA;
- Rabin.

These systems are published according to the following list:
- Fiat-Shamir, "How to prove yourself: Practical solutions to identification and signature problems", A.Odlyzko editor, Advances in Cryptology, Proc. of Crypto '86, August 11 - 15, (Lecture Notes in Computer Science 263), pp. 186 - 194, Springer Verlag, 1987, Santa Barbara, California, USA

- Feige-Fiat-Shamir, "Zero knowledge proofs of identity", Journal of Cryptology, 1(2), pp. 77 - 94, 1988

- Quisquater-Guillou, "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory", C.G. Günther editor, Advances in Cryptology, Proc. of Crypto '88, August 16 - 20, (Lecture Notes in Computer Science 330), pp. 123 - 128, Springer Verlag, 1988, Santa Barbara, California, USA

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

- Fischer-Micali-Rackoff, Unedited papers mentioned in the bibliography of Fiat-Shamir

- RSA: Rivest-Shamir-Adeleman, "A method of obtaining Digital Signatures and Public-key Cryptosystems", CACM, pp. 120 - 126, Vol. 21, No. 2, Feb. 1978

- Rabin, "Digitalized Signatures", Foundations of secure Computations, R.A. DeMillo et al. editors, Academic Press, pp. 155 - 166, London, 1987

This Sheet Has Been Replaced



* C L M S *

THIS SHEET HAS BEEN REPLACED

Claims

1. Method for secure sending of a number S = D mod X or of a set of numbers S(j) = D(j) mod X, j = 1,...,i, from a sender device (28) to a receiver device (27), whereby X is a product of at least two big prime numbers and D is greater than X, **characterized in** the following steps:
- picking a random number A or a set of random numbers A(j) by said sender device;
- calculating in said sender a value E = D+A*X or a set of values E(j) = D(j)+A(j)*X, whereby X is stored in said sender, or calculating in said sender a set of values E(j) = D(j)*B, whereby a fixed number B = A*X is stored in said sender;
- transmitting via an interface (10) said value and said values, respectively, from said sender to said receiver;
- calculating by said receiver S = E mod X or S(j) = E(j) mod X, whereby the number X is stored in said receiver device.

2. Method according to claim 1, **characterized in** that the transmitted length of value E or of each of values E(j) is less than four times the length of X.

3. Method according to claim 1 or 2, **characterized in** that the length of X is in the range from 64 to 128 bytes.

4. Method according to any of claims 1 to 3, **characterized in** that said sender device (28) calculates, using |X| cells of memory means (26), and transmits in a first step |X| lower bytes and in a second step |X| higher bytes of said value E or of each of said values E(j), whereby said receiver device (27) reconstructs said value E or of each of said values E(j) by concatenating High(E) and Low(E) or High(E(j)) and Low(E(j)).

This Sheet Has Been Replaced

5. Method according to any of claims 1 to 4, **characterized** in that said sender device (28) is a smart-card.

6. Sender apparatus (28) for a method according to any of claims 1 to 5, consisting of first computation means (25), first memory means (26) which are connected to said first computation means and first data exchange means (24) which are connected to said first computation means, whereby either
said first memory means store said modulus X and said first computation means select said random number A or random numbers A(j) and calculate said value E = D+A*X or calculate said set of values E(j) = D(j)+A(j)*X
or
said first memory means store said fixed number B and said first computation means calculate said set of values E(j) = D(j)+B
and whereby said first data exchange means (24) send said value E or said set of values E(j) to said receiver device (27).

7. Receiver apparatus (27) for a method according to any of claims 1 to 5, consisting of second computation means (22), second memory means (21) which are connected to said second computation means and second data exchange means (23) which are connected to said second computation means, whereby said second memory means store said modulus X and said second computation means calculate the modulo function S = E mod X of said value E or calculate a set of modulo functions S(j) = E(j) mod X of said set of values E(j).

8. Sender device according to claim 6, **characterized in** that said sender device (28) is a smart-card or a credit-card or a passport or a door-key.

This Sheet Has Been Replaced

9. Receiver device according to claim 7, **characterized in** that said receiver device (27) is a pay TV decoder or a credit-card verifier or a passport verifier or an electronic lock.

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

Summary

In access control systems, e.g. pay TV systems, square, or more general, d-th roots modulo X are used where X is a composite number having at least two large prime factors. If a sender, e.g. a smart-card, communicates with a receiver only few data are transmitted in order to save time. But this results in an increased number of computation operations in the sender and/or receiver.
The invention is applicable when a first cryptographic device (28) communicates with a second cryptographic device (27), especially when the devices use a modulo-based protocol. Thereby the required number of modular operations is reduced or even eliminated. It can be avoided to do modular operations by the first device.
This is particularily advantageous when said first device has a weaker computional power (e.g. less RAM and/or ROM capacity, slower clock rate) than said second device.

Fig. 2

This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

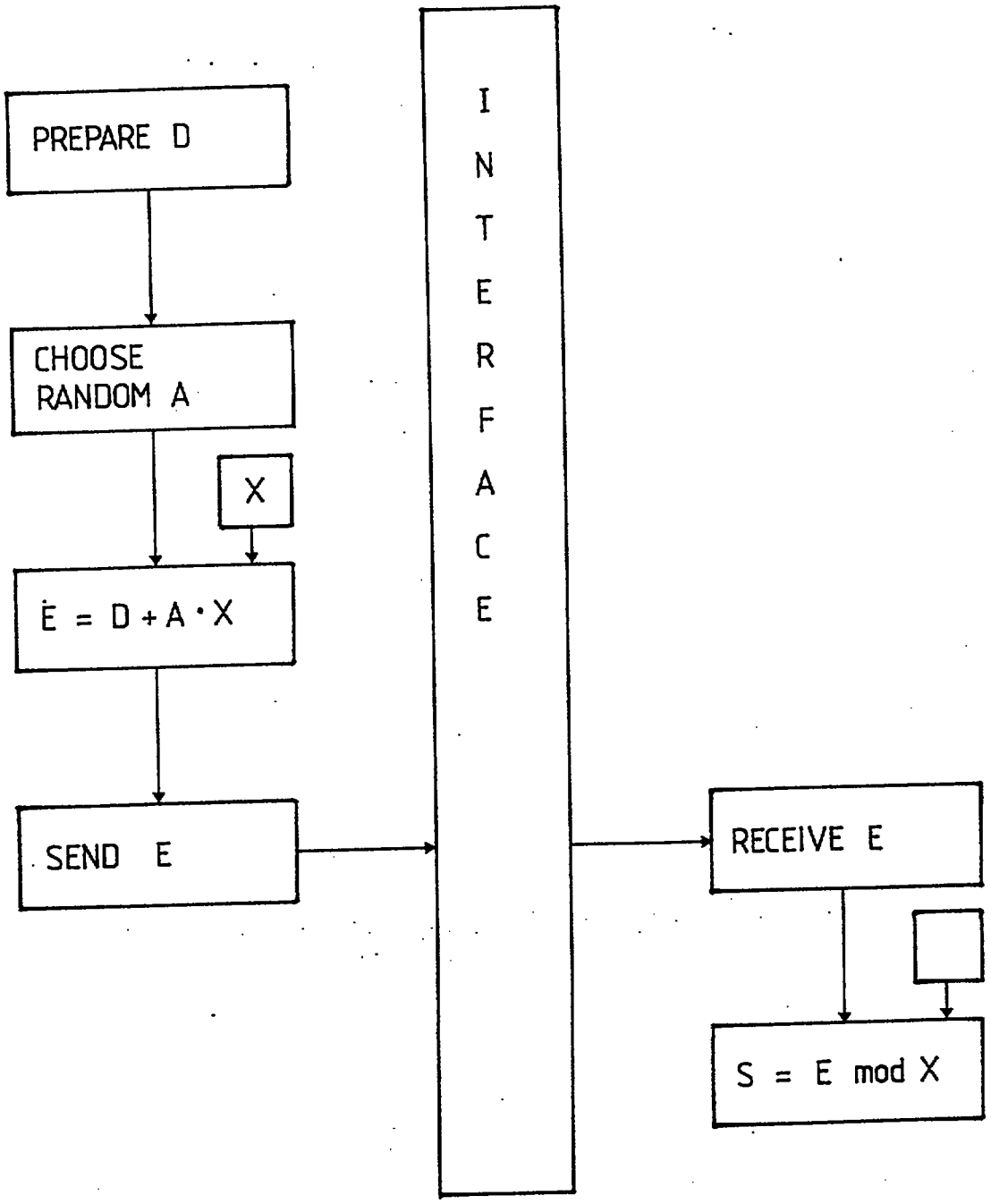


Fig.1

This Sheet Has Been Replaced

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

REPLACEMENT SHEET

0 1 MAR 1997

Method, sender apparatus and receiver apparatus for modulo operation

The present invention relates to a method, to a sender apparatus and to a receiver apparatus for modulo operation.

Background

In access control systems, e.g. pay TV systems, square, or more general, d-th roots modulo X are used where X is a composite number having at least two large prime factors. Typically the length of such a number X (denoted |X|) is 64 bytes.
If a sender, e.g. a smart-card, communicates with a receiver only few data are transmitted in order to save time. But this results in an increased number of computation operations in the sender and/or receiver.

Invention

It is one object of the invention to disclose a method for time-reduced modulo operations. This object is reached by the inventive method disclosed in claim 1.

In principle the inventive method consists in secure sending of a number S = D mod X or of a set of numbers S(j) = D(j) mod X, j = 1,...,i, from a sender device 28 to a receiver device 27, whereby X is a product of at least two big prime numbers and D is greater than X, comprising the following steps:
- picking a random number A or a set of random numbers A(j) by said sender device;
- calculating in said sender a value E = D+A*X or a set of values E(j) = D(j)+A(j)*X, whereby X is stored in said sender, or calculating in said sender a set of values E(j) =

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

REPLACEMENT SHEET
0 1 MAR 1997

D(j)*B, whereby a fixed number B = A*X is stored in said sender;
- transmitting via an interface 10 said value and said values, respectively, from said sender to said receiver;
- calculating by said receiver S = E mod X or S(j) = E(j) mod X, whereby the number X is stored in said receiver device.

Advantageous additional embodiments of the inventive method are resulting from the respective dependent claims.

It is a further object of the invention to disclose a sender apparatus which utilizes the inventive method. This object is reached by the inventive apparatus disclosed in claim 6.

In principle the inventive sender apparatus consists in first computation means 25, first memory means 26 which are connected to said first computation means and first data exchange means 24 which are connected to said first computation means, whereby either
said first memory means store said modulus X and said first computation means select said random number A or random numbers A(j) and calculate said value E = D+A*X or calculate said set of values E(j) = D(j)+A(j)*X
or
said first memory means store said fixed number B and said first computation means calculate said set of values E(j) = D(j)+B
and whereby said first data exchange means 24 send said value E or said set of values E(j) to said receiver device 27.

Advantageous additional embodiments of the inventive sender apparatus are resulting from the respective dependent claims.

It is a further object of the invention to disclose a receiver apparatus which utilizes the inventive method. This object is reached by the inventive apparatus disclosed in claim 7.

THIS SHEET HAS BEEN REPLACED

REPLACEMENT SHEET
0 1 MAR 1997

In principle the inventive receiver apparatus consists in second computation means 22, second memory means 21 which are connected to said second computation means and second data exchange means 23 which are connected to said second computation means, whereby said second memory means store said modulus X and said second computation means calculate the modulo function S = E mod X of said value E or calculate a set of modulo functions S(j) = E(j) mod X of said set of values E(j).

Advantageous additional embodiments of the inventive receiver apparatus are resulting from the respective dependent claims.

The invention is applicable when a first cryptographic device (sender) communicates with a second cryptographic device (receiver), especially when the devices use a modulo-based protocol. Thereby the required number of modular operations is reduced or even eliminated. It can be avoided to do modular operations by the first device.
This is particularly advantageous when said first device, e.g. a smart-card, has a weaker computional power (e.g. less RAM and/or ROM capacity, slower clock rate) than said second device (e.g. a powerful processor acting as a verifier).

There are such access control systems where all the numbers appearing in the first ("weaker") device have a size n*|X| bytes before modular reduction, where n is a very small integer, typically 2 or 3.
There are different variants of the inventive method.
First variant:
Let D be a number of length n*|X| bytes.
The sender wishes to communicate S = D mod X to the receiver. For avoiding the modular reduction the sender chooses a random number A, computes E = D+A*X and sends this value E to the receiver. Since A is random the value of D is hidden in E and the receiver can calculate S by:
S = E mod X, because

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

REPLACEMENT SHEET
01 MAR 1997

E mod X = D mod X + A*X mod X = D mod X.

Second variant:
The sender wishes to communicate a set of i numbers S(j) = D(j) mod X to the receiver.
Number A is a secret of the sender. The sender keeps in a ROM a pre-calculated constant B, B = A*X.
As before, let D(1),...,D(i) be a set of numbers (all bigger than X) such that the set of values S(j) is to be send to the receiver. Then these D(i) can be hidden by sending to the receiver E(1) = D(1)+B,...,E(i) = D(i)+B. The receiver will recover S(j) by calculating:
S(j) = E(j) mod X, because
E(j) mod X = D(j) mod X + B mod X = D(j) mod X.
Number i may have a value of 10.

The first and the second variant can be modified. This modification fits especially to smart-card applications. It allows the sender to perform squarings or a multiplication (which result is E) with only |X| RAM bytes.
For doing so the sender computes only the |X| lower bytes of E (denoted Low(E)) and sends them to the receiver. This computation of Low(E) requires only |X| RAM cells. After the receiver gets Low(E), the sender can reuse his |X| RAM bytes to compute the |X| higher bytes of E (denoted High(E)). When the receiver gets High(E) it calculates
E = Concatenation (High(E),Low(E))
and continues its calculations as before.

This Sheet Has Been Replaced



This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

REPLACEMENT SHEET

0 1 MAR 1997

Drawings

Preferred embodiments of the invention will now be described with reference to the accompanying drawings, in which:

Fig. 1 shows an inventive communication protocol between the sender and the receiver;
Fig. 2 shows a sender and a receiver.

Preferred embodiments

Fig. 1 shows an interface 10 between a sender, e.g. a weak processor in a smart-card, and a receiver, e.g. a pay TV decoder, which may contain a powerful processor for calculating the modulo function. The microprocessor in the sender prepares a first number D or a first set of numbers D(j). Then it chooses a random number A and calculates E = D+A*X or it adds value B to each number D(j) and sends E and the set E(j), respectively, via interface 10 to the receiver side. The receiver calculates S = E mod X or S(j) = E(j) mod X from the received numbers.
Advantageous the final length |E| or |E(j)| of E and E(j), respectively, is less than four times the length |X| of X.

In Fig. 2 a receiver device 27 and a sender device 28 are depicted. The sender device contains a first microprocessor 25, first memory means 26 which are connected to microprocessor 25 and a first connector 24 for data exchange with receiver device 27.
The receiver device 27 contains a second microprocessor 22, second memory means 21 which are connected to microprocessor 22 and a second connector 23 for data exchange with sender device 28.
First connector 24 and second connector 23 represent the interface 10 in Fig. 1. The first memory means 26 store intermediate calculation results and/or values X and/or B or

THIS SHEET HAS BEEN REPLACED

REPLACEMENT SHEET
01 MAR 1997

Low(E)/High(E). First microprocessor 25 computes data as shown in the left side of Fig. 1.
The second memory means 21 store value X and/or intermediate results. Second microprocessor 22 computes data as shown in the right side of Fig. 1.

The invention can be used for identification (VideoCrypt or EuroCrypt Pay TV system) and/or digital signature (credit cards) and/or encryption, especially together with one or more of the following systems for getting in the receiver modulo calculated results without respective modulo calculation in the sender:

- Fiat-Shamir;
- Feige-Fiat-Shamir;
- Quisquater-Guillou;
- Fischer-Micali-Rackoff;
- Naccache (EP-A-91400111, EP-A-91400301);
- RSA;
- Rabin.

These systems are published according to the following list:
- Fiat-Shamir, "How to prove yourself: Practical solutions to identification and signature problems", A.Odlyzko editor, Advances in Cryptology, Proc. of Crypto '86, August 11 - 15, (Lecture Notes in Computer Science 263), pp. 186 - 194, Springer Verlag, 1987, Santa Barbara, California, USA

- Feige-Fiat-Shamir, "Zero knowledge proofs of identity", Journal of Cryptology, 1(2), pp. 77 - 94, 1988

- Quisquater-Guillou, "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory", C.G. Günther editor, Advances in Cryptology, Proc. of Crypto '88, August 16 - 20, (Lecture Notes in Computer Science 330), pp. 123 - 128, Springer Verlag, 1988, Santa Barbara, California, USA

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

REPLACEMENT SHEET
0 1 MAR 1997

- Fischer-Micali-Rackoff, Unedited papers mentioned in the bibliography of Fiat-Shamir

- RSA: Rivest-Shamir-Adeleman, "A method of obtaining Digital Signatures and Public-key Cryptosystems", CACM, pp. 120 - 126, Vol. 21, No. 2, Feb. 1978

- Rabin, "Digitalized Signatures", Foundations of secure Computations, R.A. DeMillo et al. editors, Academic Press, pp. 155 - 166, London, 1987

This Sheet Has Been Replaced



This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

REPLACEMENT SHEET

01 MAR 1997

Claims

1. Method for secure sending of a number S = D mod X or of a set of numbers S(j) = D(j) mod X, j = 1,...,i, from a sender device (28) to a receiver device (27), whereby X is a product of at least two big prime numbers and D is greater than X, **characterized in** the following steps:
- picking a random number A or a set of random numbers A(j) by said sender device;
- calculating in said sender a value E = D+A*X or a set of values E(j) = D(j)+A(j)*X, whereby X is stored in said sender, or calculating in said sender a set of values E(j) = D(j)*B, whereby a fixed number B = A*X is stored in said sender;
- transmitting via an interface (10) said value and said values, respectively, from said sender to said receiver;
- calculating by said receiver S = E mod X or S(j) = E(j) mod X, whereby the number X is stored in said receiver device.

2. Method according to claim 1, **characterized in** that the transmitted length of value E or of each of values E(j) is less than four times the length of X.

3. Method according to claim 1 or 2, **characterized in** that the length of X is in the range from 64 to 128 bytes.

4. Method according to any of claims 1 to 3, **characterized in** that said sender device (28) calculates, using |X| cells of memory means (26), and transmits in a first step |X| lower bytes and in a second step |X| higher bytes of said value E or of each of said values E(j), whereby said receiver device (27) reconstructs said value E or of each of said values E(j) by concatenating High(E) and Low(E) or High(E(j)) and Low(E(j)).



This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

REPLACEMENT SHEET

0 1 MAR 1997

5. Method according to any of claims 1 to 4, **characterized** in that said sender device (28) is a smart-card.

6. Sender apparatus (28) for a method according to any of claims 1 to 5, consisting of first computation means (25), first memory means (26) which are connected to said first computation means and first data exchange means (24) which are connected to said first computation means, whereby either
said first memory means store said modulus X and said first computation means select said random number A or random numbers A(j) and calculate said value E = D+A*X or calculate said set of values E(j) = D(j)+A(j)*X
or
said first memory means store said fixed number B and said first computation means calculate said set of values E(j) = D(j)+B
and whereby said first data exchange means (24) send said value E or said set of values E(j) to said receiver device (27).

7. Receiver apparatus (27) for a method according to any of claims 1 to 5, consisting of second computation means (22), second memory means (21) which are connected to said second computation means and second data exchange means (23) which are connected to said second computation means, whereby said second memory means store said modulus X and said second computation means calculate the modulo function S = E mod X of said value E or calculate a set of modulo functions S(j) = E(j) mod X of said set of values E(j).

8. Sender device according to claim 6, **characterized in** that said sender device (28) is a smart-card or a credit-card or a passport or a door-key.



THIS SHEET HAS BEEN REPLACED

REPLACEMENT SHEET
01 MAR 1997

9. Receiver device according to claim 7, characterized in that said receiver device (27) is a pay TV decoder or a credit-card verifier or a passport verifier or an electronic lock.

This Sheet Has Been Replaced





REPLACEMENT SHEET
0 1 MAR 1997

METHOD, SENDER APPARATUS AND RECEIVER APPARATUS FOR MODULO OPERATION

ABSTRACT

In access control systems, e.g. pay TV systems, square, or more general, d-th roots modulo X are used where X is a composite number having at least two large prime factors. If a sender, e.g. a smart-card, communicates with a receiver only few data are transmitted in order to save time. But this results in an increased number of computation operations in the sender and/or receiver.
The invention is applicable when a first cryptographic device (28) communicates with a second cryptographic device (27), especially when the devices use a modulo-based protocol. Thereby the required number of modular operations is reduced or even eliminated. It can be avoided to do modular operations by the first device.
This is particularily advantageous when said first device has a weaker computional power (e.g. less RAM and/or ROM capacity, slower clock rate) than said second device.

Fig. 2

REPLACEMENT SHEET
0 1 MAR 1997

THIS SHEET HAS BEEN REPLACED

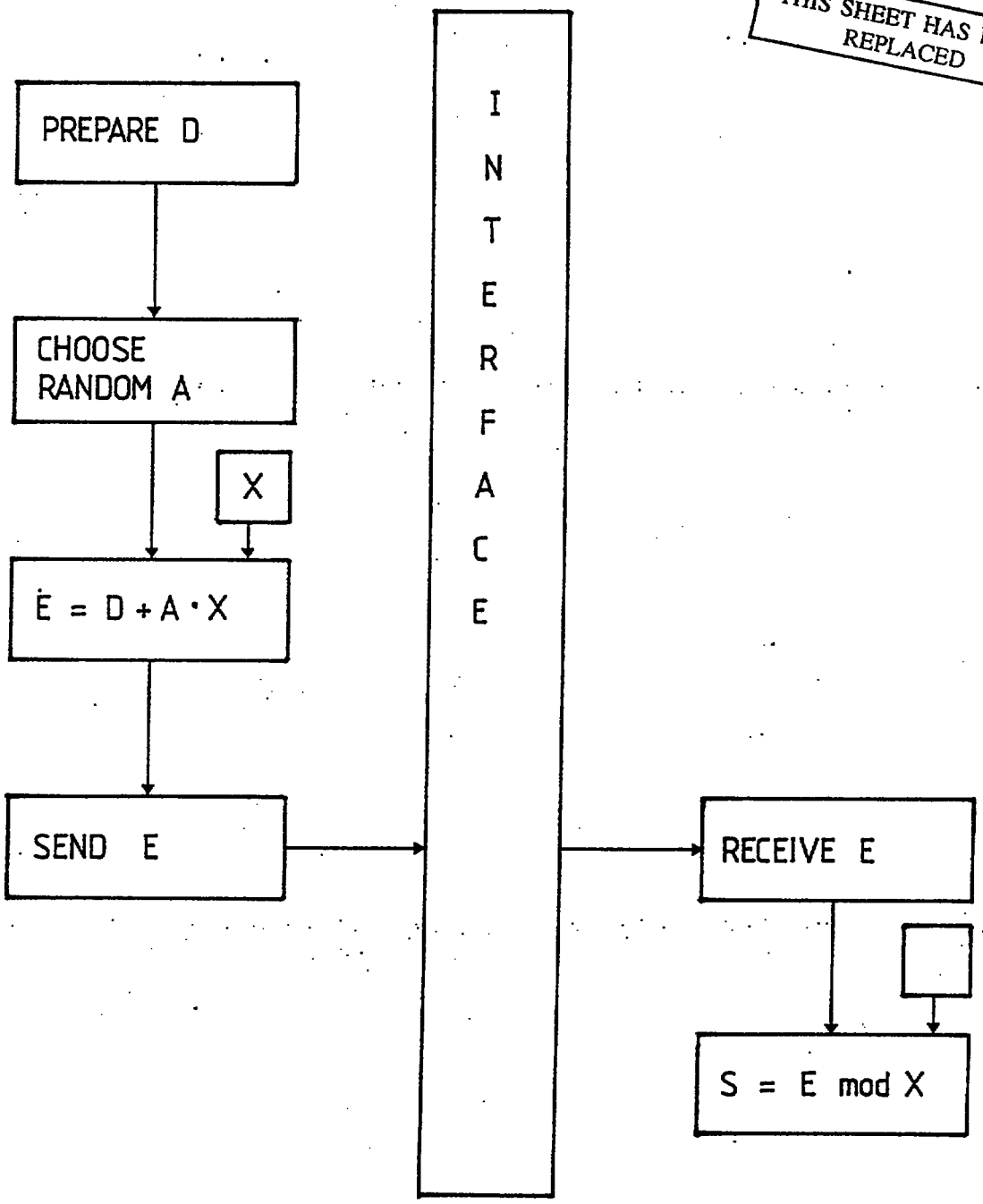


Fig.1

This Sheet Has Been Replaced

REPLACEMENT SHEET
0 1 MAR 1997

THIS SHEET HAS BEEN REPLACED

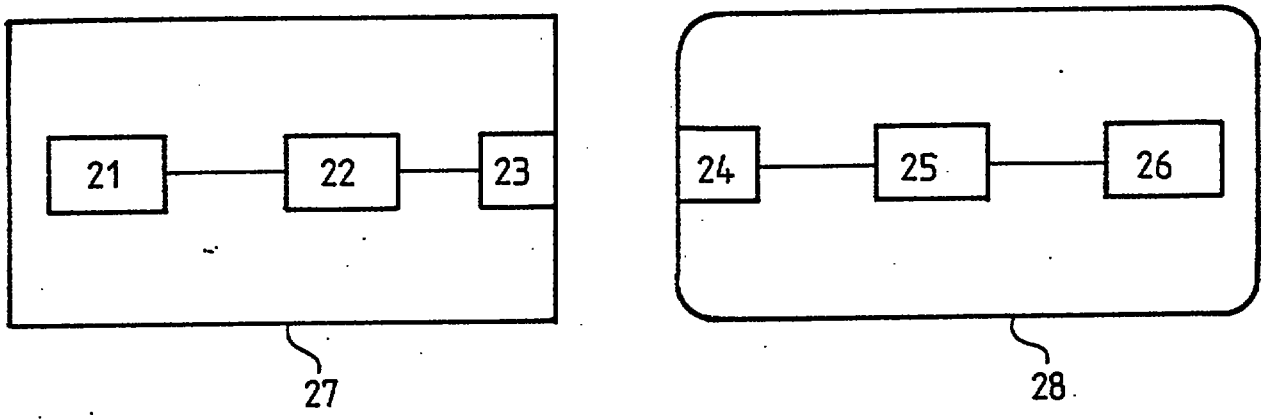


Fig.2

This Sheet Has Been Replaced

9606188-2
IPO

REPLACEMENT SHEET

18 OCT 1997

METHOD, SENDER APPARATUS AND RECEIVER APPARATUS FOR MODULO OPERATION

Description

The present invention relates to a method, to a sender apparatus and to a receiver apparatus for modulo operation.

Background

In access control systems, e.g. pay TV systems, square, or more general, d-th roots modulo X are used where X is a composite number having at least two large prime factors. Typically the length of such a number X (denoted |X|) is 64 bytes.
If a sender, e.g. a smart-card, communicates with a receiver only few data are transmitted in order to save time. But this results in an increased number of computation operations in the sender and/or receiver.

European Patent Application No. 0 428 252 discloses a system for controlling access to broadcast transmissions.

Invention

It is one object of the invention to disclose a method for time-reduced modulo operations. This object is reached by the inventive method disclosed in claim 1.

In principle the inventive method consists in secure sending of a number $S = D \bmod X$ or of a set of numbers $S(j) = D(j) \bmod X$, $j = 1,...,i$, from a sender device 28 to a receiver device 27, whereby X is a product of at least two big prime numbers and D is greater than X, comprising the following steps:

- picking a random number A or a set of random numbers A(j) by said sender device;
- calculating in said sender a value $E = D+A*X$ or a set of values $E(j) = D(j)+A(j)*X$, whereby X is stored in said sender, or calculating in said sender a set of

REPLACEMENT SHEET
18 OCT 1997

values E(j) = D(j)*B, whereby a fixed number B = A*X is stored in said sender;

- transmitting via an interface 10 said value and said values, respectively, from said sender to said receiver;
- calculating by said receiver S = E mod X or S(j) = E(j) mod X, whereby the number X is stored in said receiver device.

Advantageous additional embodiments of the inventive method are resulting from the respective dependent claims.

It is a further object of the invention to disclose a sender apparatus which utilizes the inventive method. This object is reached by the inventive apparatus disclosed in claim 6.

In principle the inventive sender apparatus consists in first computation means 25, first memory means 26 which are

connected to said first computation means and first data exchange means 24 which are connected to said first computation means, whereby either

said first memory means store said modulus X and said first computation means select said random number A or random numbers A(j) and calculate said value E = D+A*X or calculate said set of values E(j) = D(j)+A(j)*X

or

said first memory means store said fixed number B and said first computation means calculate said set of values E(j) = D(j)+B

and whereby said first data exchange means 24 send said value E or said set of values E(j) to said receiver device 27.

Advantageous additional embodiments of the inventive sender apparatus are resulting from the respective dependent claims.

It is a further object of the invention to disclose a receiver apparatus which utilizes the inventive method. This object is reached by the inventive apparatus disclosed in claim 7.

REPLACEMENT SHEET
18 OCT 1997

In principle the inventive receiver apparatus consists in second computation means 22, second memory means 21 which are connected to said second computation means and second data exchange means 23 which are connected to said second computation means, whereby said second memory means store said modulus X and said second computation means calculate the modulo function S = E mod X of said value E or calculate a set of modulo functions S(j) = E(j) mod X of said set of values E(j).

Advantageous additional embodiments of the inventive receiver apparatus are resulting from the respective dependent claims.

The invention is applicable when a first cryptographic device (sender) communicates with a second cryptographic device (receiver), especially when the devices use a modulo-based protocol. Thereby the required number of modular operations is reduced or even eliminated. It can be avoided to do modular operations by the first device.

This is particularly advantageous when said first device, e.g. a smart-card, has a weaker computional power (e. g. less RAM and/or ROM capacity, slower clock rate) than said second device (e.g. a powerful processor acting as a verifier).

There are such access control systems where all the numbers appearing in the first ("weaker") device have a size n*lXl bytes before modular reduction, where n is a very small integer, typically 2 or 3.

There are different variants of the inventive method.

First variant:

Let D be a number of length n*lXl bytes.

The sender wishes to communicate S = D mod X to the receiver. For avoiding the modular reduction the sender chooses a random number A, computes E = D+A*X and sends this value E to the receiver. Since A is random the value of D is hidden in E and the receiver can calculate S by:

$$S = E \bmod X,$$

REPLACEMENT SHEET
18 OCT 1997

because

$$E \bmod X = D \bmod X + A^*X \bmod X = D \bmod X.$$

Second variant:
The sender wishes to communicate a set of i numbers $S(j) = D(j) \bmod X$ to the receiver.
Number A is a secret of the sender. The sender keeps in a ROM a pre-calculated constant B, $B = A^*X$.
As before, let D(1),...,D(i) be a set of numbers (all bigger than X) such that the set of values S(j) is to be send to the receiver. Then these D(i) can be hidden by sending to the receiver E(1) = D(1)+B,...,E(i) = D(i)+B. The receiver will recover S(j) by calculating:

$$S(j) = E(j) \bmod X,$$

because

$$E(j) \bmod X = D(j) \bmod X + B \bmod X = D(j) \bmod X.$$

Number i may have a value of 10.

The first and the second variant can be modified. This modification fits especially to smart-card applications. It allows the sender to perform squarings or a multiplication (which result is E) with only IXI RAM bytes. For doing so the sender computes only the IXI lower bytes of E (denoted Low(E)) and sends them to the receiver. This computation of Low(E) requires only IXI RAM cells. After the receiver gets Low(E), the sender can reuse his IXI RAM bytes to compute the IXI higher bytes of E (denoted High(E)). When the receiver gets High(E) it calculates
E = Concatenation (High(E),Low(E))
and continues its calculations as before.

REPLACEMENT SHEET
18 OCT 1997

Drawings

Preferred embodiments of the invention will now be described with reference to the accompanying drawings, in which:

Fig. 1 shows an inventive communication protocol between the sender and the receiver;
Fig. 2 shows a sender and a receiver.

Preferred embodiments

Fig. 1 shows an interface 10 between a sender, e. g. a weak processor in a smart-card, and a receiver, e. g. a pay TV decoder, which may contain a powerful processor for calculating the modulo function. The microprocessor in the sender prepares a first number D or a first set of numbers D(j). Then it chooses a random number A and calculates E = D+A*X or it adds value B to each number D(j) and sends E and the set E(j), respectively, via interface 10 to the receiver side. The receiver calculates S = E mod X or S(j) = E(j) mod X from the received numbers.
Advantageous the final length |E| or |E(j)| of E and E(j), respectively, is less than four times the length |X| of X.

In Fig. 2 a receiver device 27 and a sender device 28 are depicted. The sender device contains a first microprocessor 25, first memory means 26 which are connected to microprocessor 25 and a first connector 24 for data exchange with receiver device 27.
The receiver device 27 contains a second microprocessor 22, second memory means 21 which are connected to microprocessor 22 and a second connector 23 for data exchange with sender device 28.
First connector 24 and second connector 23 represent the interface 10 in Fig. 1. The first memory means 26 store intermediate calculation results and/or values X and/or B or Low(E)/High(E). First microprocessor 25 computes data as shown in the left side of Fig. 1.

REPLACEMENT SHEET
18 OCT 1997

The second memory means 21 store value X and/or intermediate results. Second microprocessor 22 computes data as shown in the right side of Fig. 1.

The invention can be used for identification (VideoCrypt or EuroCrypt Pay TV system) and/or digital signature (credit cards) and/or encryption, especially together with one or more of the following systems for getting in the receiver modulo calculated results without respective modulo calculation in the sender:

- Fiat-Shamir;
- Feige-Fiat-Shamir;
- Quisquater-Guillou;
- Fischer-Micali-Rackoff;
- Naccache (EP-A-91400111, EP-A-91400301);
- RSA;
- Rabin.

These systems are published according to the following list:

- Fiat-Shamir, "How to prove yourself: Practical solutions to identification and signature problems", A. Odlyzko editor, Advances in Cryptology, Proc. of Crypto '86, August 11 - 15, (Lecture Notes in Computer Science 263), pp. 186 - 194, Springer Verlag, 1987, Santa Barbara, California, USA

- Feige-Fiat-Shamir, "Zero knowledge proofs of identity", Journal of Cryptology, 1(2), pp. 77 - 94, 1988

- Quisquater-Guillou, "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory", C.G. Günther editor, Advances in Cryptology, Proc. of Crypto '88, August 16 - 20, (Lecture Notes in Computer Science 330), pp. 123 - 128, Springer Verlag, 1988, Santa Barbara, California, USA

REPLACEMENT SHEET
18 OCT 1997

- RSA: Rivest-Shamir-Adeleman, "A method of obtaining Digital Signatures and Public-key Cryptosystems", CACM, pp. 120 - 126, Vol. 21, No. 2, Feb. 1978

- Rabin, "Digitalized Signatures", Foundations of secure Computations, R.A. DeMillo et al. editors, Academic Press, pp. 155 - 166, London, 1987

REPLACEMENT SHEET
18 OCT 1997

Claims

1. Method for secure sending of a number S = D mod X or of a set of numbers S(j) = D(j) mod X, j = 1,..., i, from a sender device (28) to a receiver device (27), whereby X is a product of at least two big prime numbers and D is greater than X, **characterized in** the following steps:

   - picking a random number A or a set of random numbers A(j) by said sender device;

   - calculating in said sender a value E = D+A*X or a set of values E(j) = D(j)+A(j)*X, whereby X is stored in said sender, or calculating in said sender a set of values E(j) = D(j)*B, whereby a fixed number B = A*X is stored in said sender;

   - transmitting via an interface (10) said value and said values, respectively, from said sender to said receiver;

   - calculating by said receiver S = E mod X or S (j) = E(j) mod X, whereby the number X is stored in said receiver device.

2. Method according to claim 1, **characterized in** that the transmitted length of value E or of each of values E(j) is less than four times the length of X.

3. Method according to claim 1 or 2, **characterized in** that the length of X is in the range from 64 to 128 bytes.

4. Method according to any of claims 1 to 3, **characterized in** that said sender device (28) calculates, using IXI cells of memory means (26), and transmits in a first step IXI lower bytes and in a second step

* C L M S *

REPLACEMENT SHEET
18 OCT 1997

IXI higher bytes of said value E or of each of said values E(j), whereby said receiver device (27) reconstructs said value E or of each of said values E (j) by concatenating High(E) and Low(E) or High(E (j)) and Low(E(j)).

5. Method according to any of claims 1 to 4, **characterized in** that said sender device (28) is a smartcard.

6. Sender apparatus (28) for a method according to any of claims 1 to 5 for secure sending of a number S = D mod x or of a set of numbers S(j) = D(j) mod x, j = 1,....., i, from said sender to a receiver device (27) consisting of first computation means (25), first memory means (26) which are connected to said first computation means and first data exchange means (24) which are connected to said first computation means, whereby either

   said first memory means store said modulus X and said first computation means select said random number A or random numbers A(j) and calculate said value E = D+A*X or calculate said set of values E(j) = D(j)+A(j)*X or
   said first memory means store said fixed number B and said first computation means calculate said set of values E(j) = D(j)+B
   and whereby said first data exchange means (24) send said value E or said set of values E (j) to said receiver device (27).

7. Receiver apparatus (27) for a method according to any of claims 1 to 5, consisting of second computation means (22), second memory means (21) which are connected to said second computation means and second data exchange means (23) which are connected to said second computation means, whereby said second memory means store said modulus X and said second computation means

* C L M S *

REPLACEMENT SHEET
18 OCT 1997

calculate the modulo function S = E mod X of said value E or calculate a set of modulo functions S(j) = E(j) mod X of said set of values E(j).

8. Sender device according to claim 6, **characterized in** that said sender device (28) is a smart-card or a credit-card or a passport or a door-key.

9. Receiver device according to claim 7, **characterized in** that said receiver device (27) is a pay TV decoder or a credit-card verifier or a passport verifier or an electronic lock.

* C L M S *

REPLACEMENT SHEET
18 OCT 1997

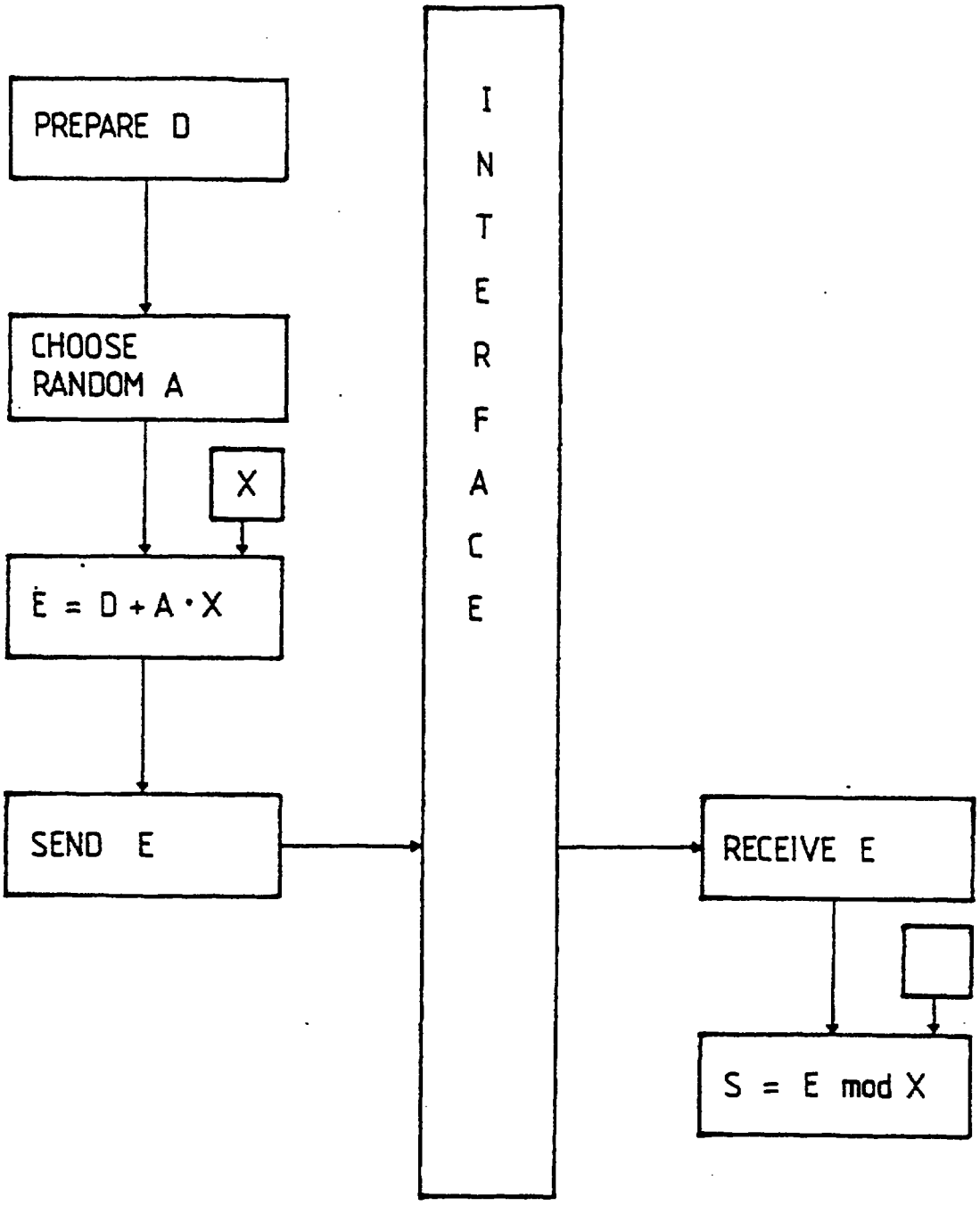


Fig.1

REPLACEMENT SHEET
18 OCT 1997

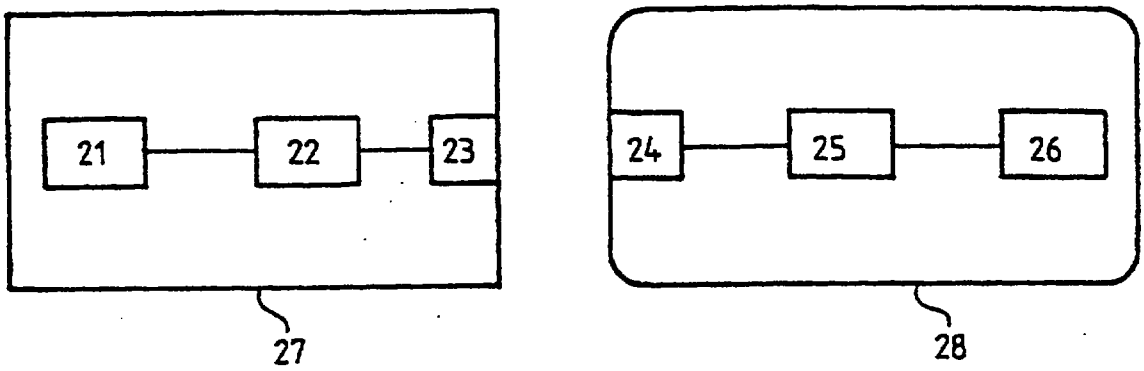


Fig. 2