US 20040120519A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2004/0120519 A1

Joye et al. (43) Pub. Date: Jun. 24, 2004

(54) METHOD FOR ENHANCING SECURITY OF PUBLIC KEY ENCRYPTION SCHEMAS

(76) Inventors: **Marc Joye**, Saint Zacharie (FR); **Jean-Sebastien Coron**, Paris (FR); **Pascal Paillier**, Cours de Vincennes (FR)

Correspondence Address:
BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404 (US)

(21) Appl. No.: **10/450,856**

(22) PCT Filed: **Nov. 20, 2001**

(86) PCT No.: **PCT/FR01/03645**

(30) **Foreign Application Priority Data**

Dec. 18, 2000 (FR) 00/16573

Publication Classification

(51) **Int. Cl.**[7] **H04K 1/00**

(52) **U.S. Cl.** **380/30**

(57) **ABSTRACT**

There exist numerous public key probabilistic encryption algorithms. Most of said algorithms do not have a maximum security level against someone capable of chosen ciphertext attacks. The method consists in a construct enabling to enhance the security of any public key probabilistic or deterministic encryption algorithm to achieve optimal security level.

METHOD FOR ENHANCING SECURITY OF PUBLIC KEY ENCRYPTION SCHEMAS

[0001] The present invention relates to a method for increasing the security of public key encryption algorithms. An encryption schema comprises an encryption algorithm and a decryption algorithm each having a particular encryption and decryption method.

[0002] In the conventional secret key cryptography model, two people wishing to communicate by means of a non-secure channel must first agree upon a secret encryption key K. The encryption function and the decryption function use the same key K. The drawback of the secret key encryption system is that said system requires prior communication of the key K between the two people by means of a secure channel, before any encrypted message is sent across the non-secure channel. In practice, it is generally difficult to find a perfectly secure communication channel, especially if the distance separating the two people is large. Secure channel means a channel for which it is impossible to know or modify the information passing through said channel. Such a secure channel can be implemented by a cable connecting two terminals, owned by said two people.

[0003] The concept of public key cryptography was invented by Whitfield Diffie and Martin Hellman in 1976. Public key cryptography makes it possible to solve the problem of distribution of keys across a non-secure channel. The principle of public key cryptography consists of using a pair of keys, a public encryption key and a private decryption key. It must be computationally impracticable to find the private decryption key from the public encryption key. A person A wishing to communicate information to a person B uses the public encryption key of person B. Only person B possesses the private key associated with their public key. Only person B is therefore capable of decrypting the message sent to them.

[0004] Another advantage of public key cryptography over secret key cryptography is that public key cryptography allows authentication through the use of electronic signing.

[0005] The first public key encryption schema implementation was devised in 1977 by Rivest, Shamir and Adleman, who invented the RSA encryption system. The security of RSA is based on the difficulty of factorising a large number which is the product of two prime numbers. Since then, numerous public key encryption systems have been proposed, the security of which is based on different computational problems (this list is not exhaustive):

[0006] Merkle-Hellman knapsack:

[0007] This encryption system is based on the difficulty of the subset sum problem.

[0008] McEliece:

[0009] This encryption system is based on algebraic code theory. It is based on the linear code decoding problem.

[0010] El-Gamal:

[0011] This encryption system is based on the difficulty of the discrete logarithm in a finite field.

[0012] Elliptical curves:

[0013] The elliptical curve encryption system constitutes a modification of existing cryptographic systems in order to apply them to the field of elliptical curves. The advantage of elliptical curve encryption systems is that they require a smaller key size than for the other encryption systems.

[0014] In the following, it is understood that all the elements necessary for the encryption schema of the invention, like for example the message M, the encrypted item C and all the abbreviations of letters or letters and numerals which follow in the description below, are integer numbers equivalent to bit strings. For example, the symbol a||b denotes the concatenation of the binary representations of the integers a and b, which are in fact the respective bit strings of a and b.

[0015] A deterministic encryption algorithm takes at the input the message M to be encrypted and returns at the output the encrypted message C.

[0016] Furthermore, a probabilistic encryption algorithm usually takes at the input the message M to be encrypted and a random number u, and returns at the output an encrypted message C, using the public key of the recipient. The decryption algorithm takes at the input the encrypted item C and returns at the output the message M, using the private key. One example of a public key probabilistic encryption algorithm is the El-Gamal encryption algorithm.

[0017] However, the majority of public key probabilistic encryption algorithms do not in themselves have a sufficient level of security. This is because there are numerous practical situations in which an attacker can have access to a data processing machine implementing the decryption algorithm using the private key. If the attacker possesses an encrypted message C, they can thus request the decryption machine to decrypt certain well-chosen encrypted messages C', different from the encrypted message C, and thus obtain information on the message M corresponding to the encrypted message C.

[0018] The method of the invention consists of a method making it possible to increase the level of security of any public key probabilistic or deterministic encryption algorithm. From a public key encryption algorithm for which an attacker cannot obtain the plain text message from the encrypted message C, a public key encryption algorithm is constructed for which an attacker cannot obtain information on the plain text message from the encrypted message C, even if the attacker has access to a machine allowing them to decrypt any encrypted message C' different from C. The construction uses in addition a secret key encryption algorithm, such that information on the message M cannot be obtained from the corresponding encrypted message C. A hybrid construction is thus obtained, making use simultaneously of a public key encryption algorithm and a secret key encryption algorithm, in order to obtain a hybrid encryption schema having a maximum level of security.

[0019] The method of the invention therefore uses a public key probabilistic or deterministic encryption schema EP taking at the input a message mp and a random number u and returning at the output an encrypted item cp. The method also uses a secret key encryption algorithm ES taking at the input a message ms and returning at the output an encrypted item cs, using a key k. The public key probabilistic or deterministic encryption algorithm uses the key pk for encrypting a message. Decryption is carried out using the corresponding private key sk.

[0020] The method of the invention comprises two distinct methods each comprising two parts:

[0021] the first method uses a probabilistic encryption algorithm and comprises two parts: the first part taking at the input the message M to be encrypted and the public key pk and returning at the output the encrypted message C; the second part is the corresponding decryption algorithm taking at the input an encrypted message C and the private key sk and returning at the output the plain text message M;

[0022] the second method uses a deterministic encryption algorithm and comprises two parts: the first part taking at the input the message M to be encrypted and the public key pk and returning at the output the encrypted message C; the second part is the corresponding decryption algorithm taking at the input an encrypted message C and the private key sk and returning at the output the plain text message M.

[0023] The first part and the second part of each of the methods of the invention also use a hash function F taking at the input a random number r and the message M, a hash function G and a hash function H.

[0024] The first part of the first method of the invention comprises the following steps:

[0025] a) Randomly generating a random number r;

[0026] b) Applying the hash function F to the message M and to the random number r in order to obtain s;

[0027] c) Applying the hash function H to s and performing an Exclusive OR of the result with r in order to obtain t;

[0028] d) Defining the intermediate message w=s||t, where || denotes the concatenation of two bit strings;

[0029] e) Applying the encryption algorithm EP to the intermediate message w and to a random number u in order to obtain **c1**, using the public key pk;

[0030] f) Applying the hash function G to w and **c1** in order to obtain k;

[0031] g) Applying the encryption algorithm ES to the message M using the key k in order to obtain the encrypted item **c2**;

[0032] h) The encrypted message C is C=**c1**||**c2**.

[0033] The second part of the first method of the invention comprises the following steps:

[0034] a) Splitting the encrypted message C into **c1** and **c2**;

[0035] b) Applying to cl a decryption algorithm EP^{-1} corresponding to the encryption algorithm EP, using a private key sk in order to obtain the intermediate message w=s||t;

[0036] c) Applying the hash function G to w and **c1** in order to obtain k;

[0037] d) Applying the decryption algorithm ES^{-1} corresponding to the encryption algorithm ES to the encrypted message **c2** using the key k in order to obtain the message M;

[0038] e) Applying the hash function H to S and performing an Exclusive OR with t in order to obtain r;

[0039] f) Applying the hash function F to the message M and to the random number r in order to obtain s';

[0040] g) Verifying that s'=s;

[0041] If s' and s are different, rejecting the encrypted message C;

[0042] Otherwise, going to step h;

[0043] h) Returning the plain text message M.

[0044] The first part of the second method of the invention comprises the following steps:

[0045] a) Randomly generating a random number r;

[0046] b) Applying the hash function F to the message M and to the random number r in order to obtain s;

[0047] c) Applying the hash function H to s and performing an Exclusive OR of the result with r in order to obtain t;

[0048] d) Defining the intermediate message w=s||t, where || denotes the concatenation of two bit strings;

[0049] e) Applying the encryption algorithm EP to the intermediate, message w in order to obtain **c1**, using the public key pk;

[0050] f) Applying the hash function G to w and **c1** in order to obtain k;

[0051] g) Applying the encryption algorithm ES to the message M using the key k in order to obtain the encrypted item **c2**;

[0052] h) The encrypted message C is C=**c1**||**c2**.

[0053] The second part of the second method of the invention comprises the following steps:

[0054] a) Splitting the encrypted message C into **c1** and **c2**;

[0055] b) Applying to **c1** a decryption algorithm EP^{-1} corresponding to the encryption algorithm EP using a private key sk in order to obtain the intermediate message w=s||t;

[0056] c) Applying the hash function G to w and **c1** in order to obtain k;

[0057] d) Applying the decryption algorithm ES^{-1} corresponding to the encryption algorithm ES to the encrypted message **c2** using the key k in order to obtain the message M;

[0058] e) Applying the hash function H to s and performing an Exclusive OR with t in order to obtain r;

[0059] f) Applying the hash function F to the message M and to the random number r in order to obtain s';

[0060] g) Verifying that s'=s;

[0061] If s' and s are different, rejecting the encrypted message C;

[0062] Otherwise, going to step h;

[0063] h) Returning the plain text message M.

[0064] Preferentially, the steps d of the first part of the two methods are replaced by the calculation w=i||s||t or w=s||i||t or w=s||t||i, where i is any value which may contain useful information like for example the binary size of the message M or the identity of the entity which encrypted M and sent the encrypted message C. Also, the secret key encryption algorithm ES is replaced in the steps g by an Exclusive OR operation between the message M to be encrypted and the key k, in order to obtain the encrypted item c**2**.

[0065] Also preferentially, the steps b of the second parts of the two methods are replaced by the operations w=i||s||t or w=s||i||t or w=s||t||i, and make it possible to deduce therefrom the value i for any calculation or verification purpose. Also, the secret key decryption algorithm ES^{-1} is replaced in the steps d by an Exclusive OR operation between the message c**2** to be encrypted and the key k, in order to obtain the encrypted item M.

[0066] The public key encryption algorithm constructed is therefore a hybrid encryption algorithm using both a public key encryption algorithm and a secret key encryption algorithm, which makes it possible to obtain better performance as regards encryption times. The public key encryption algorithm thus constructed has an optimum level of security: an attacker cannot obtain information on the plain text message M corresponding to the encrypted message C, even if they have access to a decryption machine allowing them to decrypt any message C' distinct from C.

[0067] The above-described methods of the invention are intended for portable electronic objects of the smart card type.

1. A public key encryption method taking at the input a message M to be encrypted and the public key pk and returning at the output the encrypted message C, said method using a public key probabilistic encryption algorithm EP taking at the input a message mp and a random number u and returning at the output an encrypted item cp, said method also using a secret key encryption algorithm ES taking at the input a message ms and returning at the output an encrypted item cs, said public key probabilistic encryption method using the key pk for encrypting a message, also using a hash function F taking at the input a random number r and the message M, a hash function G and a hash function H, characterised in that it comprises the following eight steps:

a) Randomly generating a random number r;

b) Applying the hash function F to the message M and to the random number r in order to obtain s;

c) Applying the hash function H to s and performing an Exclusive OR of the result with r in order to obtain t;

d) Defining the intermediate message w=s||t, where || denotes the concatenation of two bit strings;

e) Applying the encryption algorithm EP to the intermediate message w and to a random number u in order to obtain c**1**, using the public key pk;

f) Applying the hash function G to w and c**1** in order to obtain k;

g) Applying the encryption algorithm ES to the message M using the key k in order to obtain the encrypted item c**2**;

h) The encrypted message C is C=c**1**||c**2**.

2. A public key decryption method corresponding to the public key encryption method according to claim 1, said method taking at the input an encrypted message C and the private key sk, sk corresponding to the public key pk of the probabilistic encryption algorithm EP, and returning at the output the plain text message M, said method being characterised in that it comprises the following steps:

i) Splitting the encrypted message C into c**1** and c**2**;

j) Applying to cl a decryption algorithm EP^{-1} corresponding to the encryption algorithm EP, using a private key sk in order to obtain the intermediate message w=s||t;

k) Applying the hash function G to w and c**1** in order to obtain k;

l) Applying the decryption algorithm ES^{-1} corresponding to the encryption algorithm ES to the encrypted message c**2** using the key k in order to obtain the message M;

m) Applying the hash function H to s and performing an Exclusive OR with t in order to obtain r;

n) Applying the hash function F to the message M and to the random number r in order to obtain s';

o) Verifying that s'=s;

If s' and s are different, rejecting the encrypted message C;

Otherwise, going to step h;

p) Returning the plain text message M.

3. A public key encryption method taking at the input a message M to be encrypted and the public key pk and returning at the output the encrypted message C, said method using a public key deterministic encryption algorithm EP taking at the input a message mp and returning at the output an encrypted item cp, said method also using a secret key encryption algorithm ES taking at the input a message ms and returning at the output an encrypted item cs, said public key deterministic encryption method using the key pk for encrypting a message, also using a hash function F taking at the input a random number r and the message M, a hash function G and a hash function H, characterised in that it comprises the following nine steps:

i) Randomly generating a random number r;

j) Applying the hash function F to the message M and to the random number r in order to obtain s;

k) Applying the hash function H to s and performing an Exclusive OR of the result with r in order to obtain t;

l) Defining the intermediate message w=s||t, where || denotes the concatenation of two bit strings;

m) Applying the encryption algorithm EP to the intermediate message w in order to obtain c**1**, using the public key pk;

n) Applying the hash function G to w and c**1** in order to obtain k;

o) Applying the encryption algorithm ES to the message M using the key k in order to obtain the encrypted item c**2**;

p) The encrypted message C is C=c**1**||c**2**.

4. A public key decryption method corresponding to the public key encryption method according to claim 3, said method taking at the input an encrypted message C and the private key sk, sk corresponding to the public key pk of the deterministic encryption algorithm EP, and returning at the output the plain text message M, said method being characterised in that it comprises the following steps:

i) Splitting the encrypted message C into c**1** and c**2**;

j) Applying to c**1** a decryption algorithm EP^{-1} corresponding to the encryption algorithm EP, using a private key sk in order to obtain the intermediate message w=s||t;

k) Applying the hash function G to w and c**1** in order to obtain k;

l) Applying the decryption algorithm ES^{-1} corresponding to the encryption algorithm ES to the encrypted message c**2** using the key k in order to obtain the message M;

m) Applying the hash function H to s and performing an Exclusive OR with t in order to obtain r;

n) Applying the hash function F to the message M and to the random number r in order to obtain s';

o) Verifying that s'=s;

If s' and s are different, rejecting the encrypted message C;

Otherwise, going to step h;

p) Returning the plain text message M.

5. A method according to claims **1** and **3**, characterised in that the steps d are replaced by the calculation w=i||s||t or w=s||i||t or w=s||t||i, where i is any value which may contain useful information like for example the binary size of the message M or the identity of the entity which encrypted M and sent the encrypted message C.

6. A method according to claims **2** and **4**, characterised in that the steps b make it possible to obtain w=i||s||t or w=s||i||t or w=s||t||i, and deduce therefrom the value i for any calculation or verification purpose.

7. A method according to claims **1** and **3**, characterised in that the secret key encryption algorithm ES is replaced in the steps g of claim 1 and g of claim 3 by an Exclusive OR operation between the message M to be encrypted and the key k, in order to obtain the encrypted item c**2**.

8. A method according to claims **2** and **4**, characterised in that the secret key decryption algorithm ES^{-1} is replaced in the steps d of claim 2 and d of claim 4 by an Exclusive OR operation between the message c**2** to be encrypted and the key k, in order to obtain the encrypted item M.

9. A method according to any one of the preceding claims, characterised in that the method is used in a portable electronic object of the smart card type.

* * * * *