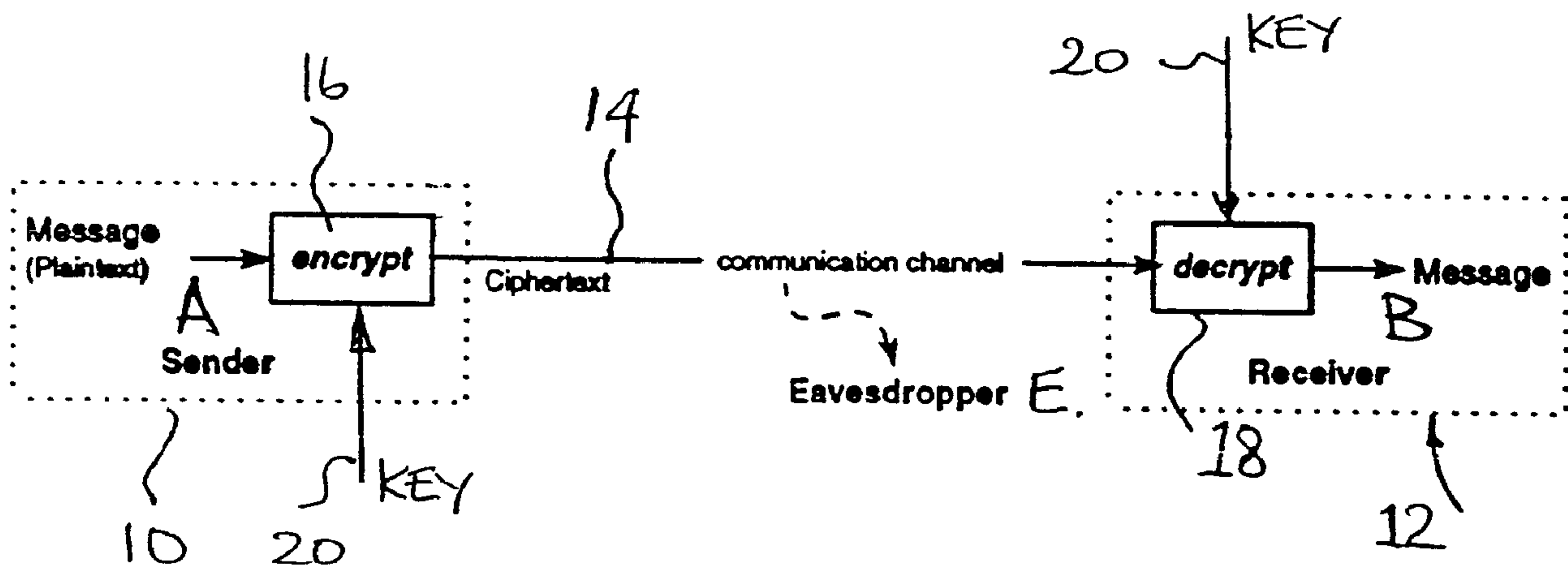




(22) Date de dépôt/Filing Date: 1996/04/16
(41) Mise à la disp. pub./Open to Public Insp.: 1996/10/22
(45) Date de délivrance/Issue Date: 2011/05/31
(62) Demande originale/Original Application: 2 174 260
(30) Priorité/Priority: 1995/04/21 (US08/426,090)

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01),
H04L 9/14 (2006.01), *H04L 9/30* (2006.01)
(72) Inventeurs/Inventors:
VANSTONE, SCOTT, CA;
MENEZES, ALFRED JOHN, CA;
QU, MINGHUA, CA
(73) Propriétaire/Owner:
CERTICOM CORP., CA
(74) Agent: BLAKE, CASSELS & GRAYDON LLP

(54) Titre : PROTOCOLE DE SELECTION ET DE TRANSFERT DE CLES
(54) Title: KEY AGREEMENT AND TRANSPORT PROTOCOL



(57) Abrégé/Abstract:

A key establishment protocol includes the generation of a value of cryptographic function, typically a hash, of a session key and public information. This value is transferred between correspondents together with the information necessary to generate the session key. Provided the session key has not been compromised, the value of the cryptographic function will be the same at each of the correspondents. The value of the cryptographic function cannot be compromised or modified without access to the session key.



ABSTRACT

A key establishment protocol includes the generation of a value of cryptographic function, typically a hash, of a session key and public information. This value is transferred between correspondents together with the information necessary to generate the session key. Provided the session key has not been compromised, the value of the cryptographic function will be the same at each of the correspondents. The value of the cryptographic function cannot be compromised or modified without access to the session key.

KEY AGREEMENT AND TRANSPORT PROTOCOL

The present invention relates to key agreement protocols for transfer and authentication of encryption keys.

5 To retain privacy during the exchange of information it is well known to encrypt data using a key. The key must be chosen so that the correspondents are able to encrypt and decrypt messages but such that an interceptor cannot determine the contents of the message.

10 In a secret key cryptographic protocol, the correspondents share a common key that is secret to them. This requires the key to be agreed upon between the correspondents and for provision to be made to maintain the secrecy of the key and provide for change of the key
15 should the underlying security be compromised.

 Public key cryptographic protocols were first proposed in 1976 by Diffie-Hellman and utilized a public key made available to all potential correspondents and a private key known only to the intended recipient. The
20 public and private keys are related such that a message encrypted with the public key of a recipient can be readily decrypted with the private key but the private key cannot be derived from the knowledge of the plaintext, ciphertext and public key.

25 Key establishment is the process by which two (or more) parties establish a shared secret key, called the session key. The session key is subsequently used to achieve some cryptographic goal, such as privacy. There are two kinds of key agreement protocol; key transport

protocols in which a key is created by one party and securely transmitted to the second party; and key agreement protocols, in which both parties contribute information which jointly establish the shared secret key. The number of message exchanges required between the parties is called the number of passes. A key establishment protocol is said to provide implicit key authentication (or simply key authentication) if one party is assured that no other party aside from a specially identified second party may learn the value of the session key. The property of implicit key authentication does not necessarily mean that the second party actually possesses the session key. A key establishment protocol is said to provide key confirmation if one party is assured that a specially identified second party actually has possession of a particular session key. If the authentication is provided to both parties involved in the protocol, then the key authentication is said to be mutual if provided to only one party, the authentication is said to be unilateral.

There are various prior proposals which claim to provide implicit key authentication.

Examples include the Nyberg-Rueppel one-pass protocol and the Matsumoto-Takashima-Imai (MTI) and the Goss and Yacobi two-pass protocols for key agreement.

The prior proposals ensure that transmissions between correspondents to establish a common key are

5 For example, the MTI/A0 key agreement protocol
establishes a shared secret K, known to the two
correspondents, in the following manner:-

- $$A \rightarrow B: \alpha^x \bmod p \quad (1)$$
- $$A \leftarrow B: \alpha^y \bmod p \quad (2)$$

The values of x and y remain secure during such transmissions as it is impractical to determine the exponent even when the value of α and the exponentiation is known provided of course that p is chosen sufficiently large.

3. To implement the protocol the following steps are performed each time a shared key is required.

- 5 (a) A chooses a random integer $x, 1 \leq x \leq p-2$, and sends B message (1) i.e. $\alpha^x \bmod p$.
- (b) B chooses a random integer $y, 1 \leq y \leq p-2$, and sends A message (2) i.e. $\alpha^y \bmod p$.
- (c) A computes the key $K = (\alpha^y)^a z_B^x \bmod p$.
- (d) B computes the key $K = (\alpha^x)^b z_A^y \bmod p$.
- 10 (e) Both share the key $K = \alpha^{bx+ay}$.

In order to compute the key K , A must use his secret key a and the random integer x , both of which are known only to him. Similarly B must use her secret key b and random integer y to compute the session key K .
 15 Provided the secret keys a, b remain uncompromised, an interloper cannot generate a session key identical to the other correspondent. Accordingly, any ciphertext will not be decipherable by both correspondents.

20 As such this and related protocols have been considered satisfactory for key establishment and resistant to conventional eavesdropping or man-in-the-middle attacks.

In some circumstances it may be advantageous
 25 for an adversary to mislead one correspondent as to the true identity of the other correspondent.

In such an attack an active adversary or interloper E modifies messages exchanged between A and B ,

with the result that B believes that he shares a key K with E while A believes that she shares the same key K with B. Even though E does not learn the value of K the misinformation as to the identity of the correspondents
5 may be useful.

A practical scenario where such an attack may be launched successfully is the following. Suppose that B is a bank branch and A is an account holder. Certificates are issued by the bank headquarters and
10 within the certificate is the account information of the holder. Suppose that the protocol for electronic deposit of funds is to exchange a key with a bank branch via a mutually authenticated key agreement. Once B has authenticated the transmitting entity, encrypted funds
15 are deposited to the account number in the certificate. If no further authentication is done in the encrypted deposit message (which might be the case to save bandwidth) then the deposit will be made to E's account.

It is therefore an object of the present
20 invention to provide a protocol in which the above disadvantages are obviated or mitigated.

According therefore to the present invention there is provided a method of authenticating a pair of correspondents A,B to permit exchange of information
25 therebetween, each of said correspondents having a respective private key a, b and a public key p_A, p_B derived from a generator α and respective ones of said private keys a, b , said method including the steps of

i) a first of said correspondents A selecting a first random integer x and exponentiating a function $f(\alpha)$ including said generator to a power $g(x)$ to provide a first exponentiated function $f(\alpha)^{g(x)}$;

5 ii) said first correspondent A forwarding to a second correspondent B a message including said first exponentiated function $f(\alpha)^{g(x)}$;

iii) said correspondent B selecting a second random integer y and exponentiating a function $f'(\alpha)$ including
10 said generator to a power $g(y)$ to provide a second exponentiated function $f'(\alpha)^{g(y)}$;

iv) said second correspondent B constructing a session key K from information made public by said first correspondent A and information that is private to said
15 second correspondent B, said session key also being constructible by said first correspondent A for information made public by B and information that is private to said first correspondent A;

v) said second correspondent B generating a value
20 h of a function $F[\pi, K]$ where $F[\pi, K]$ denotes a cryptographic function applied conjointly to π and K and where π is a subset of the public information provided by B thereby to bind the values of π and K ;

vi) said second of said correspondents B forwarding
25 a message to said first correspondent A including said second exponential function $f'(\alpha)^{g(y)}$ and said value h of said cryptographic function $F[\pi, K]$;

vii) said first correspondent receiving said message and computing a session key K' from information made public by said second correspondent B and private to said first correspondent A;

5 viii) said first correspondent A computing a value h' of a cryptographic function $h, h' = F[\pi, K']$; and

ix) comparing said values obtained from said cryptographic functions F to confirm their correspondence.

10 As the session key K can only be generated using information that is private to either A or B, the binding of K with π with the cryptographic function h prevents E from extracting K or interjecting a new value function that will correspond to that obtained by A.

15 Embodiments of the invention will now be described by way of example only with reference to the accompanying drawings in which.

Figure 1 is a schematic representation of a data communication system.

20 Referring therefore to Figure 1, a pair of correspondents, 10,12, denoted as correspondent A and correspondent B, exchange information over a communication channel 14. A cryptographic unit 16,18 is interposed between each of the correspondents 10,12 and
25 the channel 14. A key 20 is associated with each of the cryptographic units 16,18 to convert plaintext carried between each unit 16,18 and its respective correspondent 10,12 into ciphertext carried on the channel 14.

In operation, a message generated by correspondent A, 10, is encrypted by the unit 16 with the key 20 and transmitted as ciphertext over channel 14 to the unit 18.

5 The key 20 operates upon the ciphertext in the unit 18 to generate a plaintext message for the correspondent B, 12. Provided the keys 20 correspond, the message received by the correspondent 12 will be that sent by the correspondent 10.

10 In order for the system shown in Figure 1 to operate it is necessary for the keys 20 to be identical and therefore a key agreement protocol is established that allows the transfer of information in a public manner to establish the identical keys. A number of
15 protocols are available for such key generation and embodiments of the present invention will be described below in the context of modifications of existing protocols.

A commonly used set of protocols are
20 collectively known as the Matsumoto-Takashima-Imai or "MTI" key agreement protocols, and are variants of the Diffie-Hellman key exchange. Their purpose is for parties A and B to establish a secret session key K.

The system parameters for these protocols are a
25 prime number p and a generator α of the multiplicative group Z_p^* . Correspondent A has private key a and public key $p_A = \alpha^a$. Correspondent B has private key b and public key $p_B = \alpha^b$. In all four protocols exemplified below,

text_A refers to a string of information that identifies party A. If the other correspondent B possesses an authentic copy of correspondent A's public key, then text_A will contain A's public-key certificate, issued by a trusted center; correspondent B can use his authentic copy of the trusted center's public key to verify correspondent A's certificate, hence obtaining an authentic copy of correspondent A's public key.

In each example below it is assumed that an interloper E wishes to have messages from A identified as having originated from E herself. To accomplish this, E selects a random integer e , $1 \leq e \leq p-2$, computes $p_E = (p_A)^e = \alpha^e \bmod p$, and gets this certified as her public key. E does not know the exponent ae , although she knows e . By substituting text_E for text_A, the correspondent B will assume that the message originates from E rather than A and use E's public key to generate the session key K . E also intercepts the message from B and uses his secret random integer e to modify its contents. A will then use that information to generate the same session key allowing A to communicate with B.

The present invention is exemplified by modifications to 4 of the family of MTI protocols which foil this new attack thereby achieving the desired property of mutual implicit authentication. In the modified protocols exemplified below $F(X,Y)$ denotes a cryptographic function applied to a string derived from x and y . Typically and as exemplified a hash function,

such as the NIST "Secure Hash Algorithm"(SHA-1), is applied to the string obtained by concatenating X and Y but it will be understood that other cryptographic functions may be used.

5 Example 1 - MTI/A0 protocol

The existing protocol operates as follows:-

1. Correspondent A generates a random integer x , $1 \leq x \leq p-2$, computes α^x , and sends $\{\alpha^x, \text{text}_A\}$ to party B.
- 10 2. Correspondent B generates a random integer y , $1 \leq y \leq p-2$, computes α^y , and sends $\{\alpha^y, \text{text}_B\}$ to party A.
3. Correspondent A computes $K = (\alpha^y)^x (p_B)^x = \alpha^{xy+bx}$.
4. Correspondent B computes $K = (\alpha^x)^y (p_A)^y = \alpha^{xy+bx}$.

15

A common key K is thus obtained. However, with this arrangement, interloper E may have messages generated by correspondent A identified as having originated from E in the following manner.

- 20 1. E intercepts A's message $\{\alpha^x, \text{text}_A\}$ and replaces it with $\{\alpha^x, \text{text}_E\}$. The provision of the message text_E identifies the message as having originated at E.
2. B sends $\{\alpha^y, \text{text}_B\}$ to E, who then forwards
- 25 $\{(\alpha^y)^c, \text{text}_B\}$ to A. Since A receives text_B , he assumes the message originates at B and, as he does not know the value of y , assumes that α^{yc} is valid information.

3. A computes $K = (\alpha^y)^a (p_B)^x = \alpha^{ay+bx}$.
4. B computes $K = (\alpha^x)^b (p_E)^y = \alpha^{ay+bx}$.
5. A and B now share the key K, even though B believes he shares a key with E.

5

Accordingly any further transactions from A to B will be considered by B to have originated at E. B will act accordingly crediting instruction to E. Even though the interloper E does not learn the value of the session key K nevertheless the assumption that the message originates at E may be valuable and achieve the desired effect.

To avoid this problem, the protocol is modified as follows:-

- 15 1. A generates a random integer $x, 1 \leq x \leq p-2$, computes α^x , and sends $\{\alpha^x, \text{text}_A\}$ to party B.
2. B generates a random integer $y, 1 \leq y \leq p-2$, and computes α^y , $K = (\alpha^x)^b (p_A)^y = \alpha^{ay+bx}$, and a value h of cryptographic hash function $F(\alpha^y, \alpha^{ay+bx})$ which is a function of public information π and the key K. B sends $\{\alpha^y, h, \text{text}_B\}$ to party A.
- 20 3. A computes $K = (\alpha^y)^a (p_B)^x = \alpha^{ay+bx}$. A also computes a value h' of cryptographic hash function $F(\alpha^y, K)$ and verifies that this value is equal to h.
- 25

If E attempts to interpose her identification, text_E , the attack fails on the modified protocols because

in each case B sends the hash value $F(\pi, K)$, where π is B's random exponential, α^y , thereby binding together the values of π and K . E cannot subsequently replace the value of π with π^e and compute $F(\pi^e, K)$ since E does not
 5 know K . Even though E knows α^y , this is not sufficient to extract K from the hash value h . Accordingly, even if E interposes the value α^{ye} so that the keys 20 will agree, the values h, h' will not.

10 Example 2 - MTI/B0 protocol

In this protocol,

1. A generates a random integer $x, 1 \leq x \leq p-2$, computes $(p_B)^x = \alpha^{bx}$, and sends $\{\alpha^{bx}, \text{text}_A\}$ to party B.
- 15 2. B generates a random integer $y, 1 \leq y \leq p-2$, computes $(p_A)^y = \alpha^{ay}$, and sends $\{\alpha^{ay}, \text{text}_B\}$ to party A.
3. A computes $K = (\alpha^{ay})^{a^{-1}} \alpha^x = \alpha^{x+y}$
4. B computes $K = (\alpha^{bx})^{b^{-1}} \alpha^y = \alpha^{x+y}$

20

This protocol is vulnerable to the interloper E if,

1. E replaces A's message $\{\alpha^{bx}, \text{text}_A\}$ with $\{\alpha^{bx}, \text{text}_E\}$ to identify herself as the originator to the message.
- 25 2. B sends $\{(p_E)^y, \text{text}_B\}$ to E, who then computes $((P_E)^y)^{e^{-1}} = \alpha^{ey}$ and forwards $\{\alpha^{ey}, \text{text}_B\}$ to A.

3. A computes $K = (\alpha^{ay})^{a^{-1}} \alpha^x = \alpha^{x+y}$
4. B computes $K = (\alpha^{bx})^{b^{-1}} \alpha^y = \alpha^{x+y}$
5. A and B now share the key K, even though B believes he shares a key with E.

5

This protocol may be modified to resist E's attack as follows.

1. A generates a random integer $x, 1 \leq x \leq p-2$, computes $(p_B)^x = \alpha^{bx}$, and sends $\{\alpha^{bx}, \text{text}_A\}$ to party B.
2. B generates a random integer $y, 1 \leq y \leq p-2$, and computes $(p_A)^y = \alpha^{ay}$, $K = (\alpha^{bx})^{b^{-1}} \alpha^y = \alpha^{x+y}$, and the value h of hash function $F(\alpha^{ay}, \alpha^{x+y})$. B sends $\{\alpha^{ay}, h, \text{text}_B\}$ to A.
3. A computes $K = (\alpha^{ay})^{a^{-1}} \alpha^x = \alpha^{x+y}$. A also computes the value h' of hash function $F(\alpha^{ay}, K)$ and verifies that this value is equal to h .

10

15

Once again, E cannot determine the session key K and so cannot generate a new value of the hash function to maintain the deception.

20

Example 3 - MTI/CO protocol

This protocol operates as follows:-

1. A generates a random integer $x, 1 \leq x \leq p-2$, computes $(p_B)^x = \alpha^{bx}$, and sends $\{\alpha^{bx}, \text{text}_A\}$ to party B.
2. B generates a random integer $y, 1 \leq y \leq p-2$, computes $(p_A)^y = \alpha^{ay}$, and sends $\{\alpha^{ay}, \text{text}_B\}$ to party A.

25

14

3. A computes $K = (\alpha^{ay})^{a^{-1}x} = \alpha^{xy}$
4. B computes $K = (\alpha^{bx})^{b^{-1}y} = \alpha^{xy}$

The interloper E may interpose her identity as follows:-

- 5 1. E replaces A's message $\{\alpha^{bx}, \text{text}_A\}$ with $\{\alpha^{bx}, \text{text}_E\}$.
2. B sends $\{(p_E)^y, \text{text}_B\}$ to E, who then computes $((p_E)^y)^{e^{-1}} = \alpha^{ey}$ and forwards $\{\alpha^{ey}, \text{text}_B\}$ to A.
3. A computes $K = (\alpha^{ey})^{a^{-1}x} = \alpha^{xy}$
- 10 4. B computes $K = (\alpha^{bx})^{b^{-1}y} = \alpha^{xy}$
5. A and B now share the key K, even though B believes he shares a key with E.

To avoid this attack protocol is modified as follows:-

- 15 1. A generates a random integer $x, 1 \leq x \leq p-2$, computes $(p_B)^x = \alpha^{bx}$, and sends $\{\alpha^{bx}, \text{text}_A\}$ to party B.
2. B generates a random integer $y, 1 \leq y \leq p-2$, and computes $(p_A)^y = \alpha^{ay}$, $K = (\alpha^{bx})^{b^{-1}y} = \alpha^{xy}$, and value h of hash function $F(\alpha^{ay}, \alpha^{xy})$. B sends
- 20 $\{\alpha^{ay}, h, \text{text}_B\}$ to party A.
3. A computes $K = (\alpha^{ay})^{a^{-1}x} = \alpha^{xy}$. A also computes the value h' of $F(\alpha^{ay}, K)$ and verifies that this value is equal to h .

25

Example 4 - MTI/C1 protocol

In this protocol:-

1. A generates a random integer $x, 1 \leq x \leq p-2$,
computes $(p_B)^{ax} = \alpha^{abx}$, and sends $\{\alpha^{abx}, \text{text}_A\}$ to
5 party B.
2. B generates a random integer $y, 1 \leq y \leq p-2$,
computes $(p_A)^{by} = \alpha^{aby}$, and sends $\{\alpha^{aby}, \text{text}_B\}$ to
party A.
3. A computes $K = (\alpha^{aby})^x = \alpha^{abxy}$.
- 10 4. B computes $K = (\alpha^{abx})^y = \alpha^{abxy}$.

E can act as an interloper as follows:-

1. E replaces A's message $\{\alpha^{abx}, \text{text}_A\}$ with
 $\{\alpha^{abx}, \text{text}_E\}$.
- 15 2. B sends $\{(p_E)^{by}, \text{text}_B\}$ to E, who then computes
 $((p_E)^{by})^{c-1} = \alpha^{aby}$ and forwards $\{\alpha^{aby}, \text{text}_B\}$ to A.
3. A computes $K = (\alpha^{aby})^x = \alpha^{abxy}$.
4. B computes $K = (\alpha^{abx})^y = \alpha^{abxy}$.
5. A and B now share the key K, even though B
20 believes he shares a key with E.

To avoid this, the protocol is modified as follows:-

1. A generates a random integer $x, 1 \leq x \leq p-2$,
computes $(p_B)^{ax} = \alpha^{abx}$, and sends $\{\alpha^{abx}, \text{text}_A\}$ to
25 party B.
2. B generates a random integer $y, 1 \leq y \leq p-2$, and
computes $(p_A)^{by} = \alpha^{aby}, K = (\alpha^{abx})^y = \alpha^{abxy}$, and

$h = F(\alpha^{aby}, \alpha^{abxy})$. B sends $\{\alpha^{aby}, h, \text{text}_B\}$ to party A.

3. A computes $K = (\alpha^{aby})^x = \alpha^{abxy}$. A also computes $h' = F(\alpha^{aby}, K)$ and verifies that this value is equal to h .

5

In each of the modified protocols discussed above, key confirmation from B to A is provided.

As noted above instead of F being a cryptographic hash function other functions could be used. For example, an option available is to choose $F = \epsilon_K$, where ϵ is the encryption function of a suitable symmetric-key encryption scheme, and K is the session key established. Because E cannot generate the session key K , it is similarly not able to generate the value of the function F and therefore cannot interpose for the correspondent A.

The technique described above can be applied to other similar key exchange protocols, including all of the 3 infinite classes of MTI protocols called MTI-A(k), MTI-B(k) and MTI-C(k).

The Goss authenticated key exchange protocol is similar to the MTI/A0 protocol, except that the session key is the bitwise exclusive-OR of α^{ay} and α^{bx} ; that is $K = \alpha^{ay} \oplus \alpha^{bx}$ instead of being the product of α^{ay} and α^{bx} . Hence the attack on the MTI/A0 protocol and its modification can be extended in a straightforward manner to the case of the Goss protocol.

25

Similarly Yacobi's authenticated key exchange protocol is exactly the same as the MTI/A0 protocol, except that α is an element of the group of units $\mathbb{Z}_n^*$, where n is the product of 2 large primes. Again, the
5 attack on the MTI/A0 protocol and its modification can be extended in a straightforward manner to the case of the Goss protocol.

A further way of foiling the interposition of E is to require that each entity prove to a trusted center
10 that it knows the exponent of α that produces its public key P , before the center issues a certificate for the public key. Because E only knows " e " and not " ae " it would not meet this requirement. This can be achieved through zero knowledge techniques to protect the secrecy
15 of the private keys but also requires the availability of a trusted centre which may not be convenient.

Each of the above examples has been described with a 2 pass protocol for key authentication. One pass protocols also exist to establish a key between
20 correspondents and may be similarly vulnerable.

As an example the Nyberg-Rueppel one pass key agreement protocol will be described and a modification proposed.

The purpose of this protocol is for party A and
25 party B to agree upon a secret session key K .

The system parameters for these protocols are a prime number p and a generator α of the multiplicative group $\mathbb{Z}_p^*$. User A has private key a and public key

$p_A = \alpha^a$. User B has private key b and public key $p_B = \alpha^b$.

1. A selects random integers x and t , $1 \leq x, t \leq p-2$.
2. A computes $r = (p_B)^t \alpha^x \bmod p$ and $s = x - ra \bmod (p-1)$, and sends $\{r, s, \text{text}_A\}$ to B.
- 5 3. B recovers the value $\alpha^x \bmod p$ by computing $\alpha^s (p_A)^r \bmod p$ and then computes the shared session key $K = (r\alpha^x)^{b^{-1}} = \alpha^t \bmod p$.

If interloper E wishes to have messages from A identified as having originated from herself, E selects a random integer e , $1 \leq e \leq p-2$, computes $p_E = \alpha^e$, and gets this certified as her public key.

1. E intercepts A's message $\{r, s, \text{text}_A\}$ and computes $\alpha^x = \alpha^s (p_A)^r$ and $\alpha^{bt} = r\alpha^x$.
- 15 2. E then selects a random integer x' , $1 \leq x' \leq p-2$, computes $r' = \alpha^{bt} \alpha^{-x'} \bmod p$ and $s' = x' - r'e \bmod (p-1)$.
3. E sends $\{r', s', \text{text}_E\}$ to B.
4. B recovers the value $\alpha^{kt} \bmod p$ by computing $\alpha^{s'} (p_E)^{r'} \bmod p$ and then computes $K = (r'\alpha^{x'})^{b^{-1}} = \alpha^t \bmod p$.
- 20 5. A and B now share the key K , even though B believes he shares a key with E.

25 To foil such an attack the protocol is modified by requiring A to also transmit a value h of $F(p_A, K)$, where F is a hash function, an encryption function of a symmetric-key system with key K or other suitable

cryptographic function. The modified protocol is the following.

1. A selects random integers x and t , $1 \leq x, t \leq p-2$.
2. A computes $r = (p_B)^t \alpha^x \bmod p$, $s = x - ra \bmod (p-1)$, session key $K = \alpha^t \bmod p$ and the value h of hash function $F(p_A, K)$. A sends $\{r, s, h, \text{text}_A\}$ to B.
3. B recovers the value $\alpha^t \bmod p$ by computing $\alpha^s (p_A)^r \bmod p$ and then computes the shared session key $K = (r\alpha^x)^{b^{-1}} = \alpha^t \bmod p$. B also computes the value h' of function $F(p_A, K)$ and verifies that this value is equal to h .

Again therefore by binding together the public information π and the session key K in the hash function, the interposition of E will not result in identical hash functions h, h' .

In each case it can be seen that a relatively simple modification to the protocols involving the binding of public and private information in a cryptographic function foils the interposition of interloper E .

All the protocols discussed above have been described in the setting of the multiplicative group $\mathbb{Z}_p^*$. However, they can all be easily modified to work in any finite group in which the discrete logarithm problem appears intractable. Suitable choices include the multiplicative group of a finite field (in particular the finite field $\text{GF}(2^n)$), subgroups of $\mathbb{Z}_p^*$ of order q , and the

group of points on an elliptic curve defined over a finite field. In each case an appropriate generator α will be used to define the public keys.

The protocols discussed above can also be
5 modified in a straightforward way to handle the situation when each user picks their own system parameters p and α (or analogous parameters if a group other than $\mathbb{Z}_p^*$ is used).

Claims:

1. A system for authenticating a pair of correspondents to permit exchange of information therebetween, said system including a first correspondent A having a first cryptographic unit, a private key a , and a public key p_a derived from a generator α and said private key a , and a second correspondent B having a second cryptographic unit, a private key b , and a public key p_b derived from said generator α and said private key b , said system being configured to perform operations comprising:
 - i) said first cryptographic unit selecting a first random integer x and exponentiating a first function $f(\alpha)$, including said generator α , to a power $g(x)$ to provide a first exponentiated function $f(\alpha)^{g(x)}$;
 - ii) said first cryptographic unit forwarding to said second cryptographic unit a first message including said first exponentiated function $f(\alpha)^{g(x)}$;
 - iii) said second cryptographic unit selecting a second random integer y and exponentiating a second function $f'(\alpha)$, including said generator α , to a power $g(y)$ to provide a second exponentiated function $f'(\alpha)^{g(y)}$;
 - iv) said second cryptographic unit computing a session key K from information made public by said first correspondent A and from information that is private to said second correspondent B; said session key K also being computable by said first correspondent A from information made public by said second correspondent B and from information that is private to said first correspondent A;
 - v) said second cryptographic unit generating a value h of a function $F[\pi, K]$, wherein $F[\pi, K]$ denotes a cryptographic function applied conjointly to π and K to thereby bind the values of π and K , and wherein π is obtained from at least information made public by one of said second correspondent B and said first correspondent A;

vi) said second cryptographic unit forwarding to said first cryptographic unit a second message including said second exponentiated function $f'(\alpha)^{g(y)}$ and said value h of said cryptographic function $F[\pi, K]$;

vii) said first cryptographic unit receiving said second message and computing a corresponding session key K' from said information made public by said second correspondent B and said information that is private to said first correspondent A;

viii) said first cryptographic unit computing a corresponding value h' of a corresponding cryptographic function $F[\pi, K']$; and

ix) said first cryptographic unit comparing said value h with said corresponding value h' to confirm their correspondence.

2. The system according to claim 1 wherein said first message includes an identification of said first correspondent A.

3. The system according to claim 1 or claim 2 wherein said second message includes an identification of said second correspondent B.

4. The system according to any one of claims 1 to 3 wherein said first function $f(\alpha)$, including said generator α , is said generator α .

5. The system according to claim 4 wherein said second function $f'(\alpha)$, including said generator α , is said generator α .

6. The system according to any one of claims 1 to 3 wherein said first function $f(\alpha)$, including said generator α , includes said public key p_b of said second correspondent B.

7. The system according to claim 6 wherein said second function $f'(\alpha)$, including said generator α , includes said public key p_a of said first correspondent A.

8. The system according to any one of claims 1 to 7 wherein said cryptographic function $F[\pi, K]$ is a cryptographic hash of π and K , and said corresponding cryptographic function $F[\pi, K']$ is a cryptographic hash of π and K' .

9. The system according to claim 7 wherein said session key K computed by said second cryptographic unit is of the form $K = (p_b^{ax})^y$ and said corresponding session key K' computed by said first cryptographic unit is of the form $K' = (p_a^{by})^x$.
10. The system according to claim 7 wherein said session key K computed by said second cryptographic unit is of the form $K = (p_b^x)^{b^{-1}y}$ and said corresponding session key K' computed by said first cryptographic unit is of the form $K' = (p_a^y)^{a^{-1}x}$.
11. The system according to claim 7 wherein said session key K computed by said second cryptographic unit is of the form $K = (p_b^x)^{b^{-1}} (\alpha)^y$ and said corresponding session key K' computed by said first cryptographic unit is of the form $K' = (p_a^y)^{a^{-1}} (\alpha)^x$.
12. The system according to claim 5 wherein said session key K computed by said second cryptographic unit is of the form $K = (\alpha^x)^b (p_a)^y$ and said corresponding session key K' computed by said first cryptographic unit is of the form $K' = (\alpha^y)^a (p_b)^x$.
13. The system according to any one of claims 1 to 12 wherein said information made public by one of said second correspondent B and said first correspondent A is information made public by said second correspondent.
14. The system according to any one of claims 1 to 13 wherein said system is an elliptic curve cryptographic system based on an underlying elliptic curve group.
15. A method for authenticating a first correspondent A and a second correspondent B to permit exchange of information therebetween, said first correspondent A having a cryptographic unit, a private key a , and a public key p_a derived from a generator α and said private key a , said method comprising:
 - i) said cryptographic unit selecting a first random integer x and exponentiating a first function $f(\alpha)$, including said generator α , to a power $g(x)$ to provide a first exponentiated function $f(\alpha)^{g(x)}$;

- ii) said cryptographic unit forwarding to said second correspondent B a first message including said first exponentiated function $f(\alpha)^{g(x)}$;
- iii) said cryptographic unit receiving from said second correspondent B a second message including: (a) a value h of a function $F[\pi, K]$ wherein $F[\pi, K]$ denotes a cryptographic function applied conjointly to π and K to thereby bind the values of π and K , wherein π was obtained from at least information made public by one of said first correspondent A and said second correspondent B, and K is a session key constructed by said second correspondent B using information made public by said first correspondent A and information that is private to said second correspondent B; and (b) a second exponentiated function $f'(\alpha)^{g(y)}$ wherein y is a second random integer that was generated by said second correspondent B;
- iv) said cryptographic unit computing a corresponding session key K' from said information made public by said second correspondent B and information that is private to said first correspondent A;
- v) said cryptographic unit computing a corresponding value h' of a corresponding cryptographic function $F[\pi, K']$; and
- vi) said cryptographic unit comparing said value h with said corresponding value h' to confirm their correspondence.

16. The method according to claim 15 wherein said first message includes an identification of said first correspondent A.

17. The method according to claim 15 or claim 16 wherein said second message includes an identification of said second correspondent B.

18. The method according to any one of claims 15 to 17 wherein said first function $f(\alpha)$, including said generator α , is said generator α .

19. The method according to any one of claims 15 to 17 wherein said first function $f(\alpha)$, including said generator α , includes a public key p_b of said second correspondent B.

20. The method according to any one of claims 15 to 19 wherein said cryptographic function $F[\pi, K]$ is a cryptographic hash of π and K , and said corresponding cryptographic function $F[\pi, K']$ is a cryptographic hash of π and K' .
21. The method according to claim 19 wherein said corresponding session key K' computed by said cryptographic unit is of the form $K' = (p_a^{by})^x$.
22. The method according to claim 19 wherein said corresponding session key K' computed by said cryptographic unit is of the form $K' = (p_a^y)^{a^{-1}x}$.
23. The method according to claim 19 wherein said corresponding session key K' computed by said cryptographic unit is of the form $K' = (p_a^y)^{a^{-1}}(\alpha)^x$.
24. The method according to claim 18 wherein said corresponding session key K' computed by said cryptographic unit is of the form $K' = (\alpha^y)^a(p_b)^x$.
25. The method according to any one of claims 15 to 24 wherein said information made public by one of said second correspondent B and said first correspondent A is information made public by said second correspondent B.
26. The method according to any one of claims 15 to 25 wherein said method includes operations based on an underlying elliptic curve group.
27. A method for authenticating a first correspondent A and a second correspondent B to permit exchange of information therebetween, said second correspondent B having a cryptographic unit, a private key b , and a public key p_b derived from a generator α and said private key b , said method comprising:
- i) said cryptographic unit receiving from said first correspondent A a first message including a first exponentiated function $f(\alpha)^{g(x)}$, wherein x is a first random number that was generated by said first correspondent A;

ii) said cryptographic unit selecting a second random integer y and exponentiating a second function $f'(\alpha)$, including said generator α , to a power $g(y)$ to provide a second exponentiated function $f'(\alpha)^{g(y)}$;

iii) said cryptographic unit constructing a session key K from information made public by said first correspondent A and from information that is private to said second correspondent B; said session key K also being constructible by said first correspondent A from information made public by said second correspondent B and from information that is private to said first correspondent A;

iv) said cryptographic unit generating a value h of a function $F[\pi, K]$ wherein $F[\pi, K]$ denotes a cryptographic function applied conjointly to π and K to thereby bind the values of π and K , and wherein π is obtained from at least information made public by one of said first correspondent A and said second correspondent B; and

v) said cryptographic unit forwarding to said first correspondent A a second message including said second exponentiated function $f'(\alpha)^{g(y)}$ and said value h ; whereby said first correspondent A can compute a corresponding session key K' from said information made public by said second correspondent B and said information that is private to said first correspondent A, and said first correspondent A can compute a corresponding value h' of a corresponding cryptographic function $F[\pi, K']$ and can compare said value h with said corresponding value h' to confirm their correspondence.

28. The method according to claim 27 wherein said first message includes an identification of said first correspondent A.

29. The method according to claim 27 or claim 28 wherein said second message includes an identification of said second correspondent B.

30. The method according to any one of claims 27 to 29 wherein said second function $f'(\alpha)$, including said generator α , is said generator α .

31. The method according to any one of claims 27 to 29 wherein said second function $f'(\alpha)$, including said generator α , includes a public key p_a of said first correspondent A.

32. The method according to any one of claims 27 to 31 wherein said cryptographic function $F[\pi, K]$ is a cryptographic hash of π and K .
33. The method according to claim 31 wherein said session key K computed by said second cryptographic unit is of the form $K = (p_b^{\alpha x})^y$.
34. The method according to claim 31 wherein said session key K computed by said second cryptographic unit is of the form $K = (p_b^x)^{b^{-1}y}$.
35. The method according to claim 31 wherein said session key K computed by said second cryptographic unit is of the form $K = (p_b^x)^{b^{-1}}(\alpha)^y$.
36. The method according to claim 30 wherein said session key K computed by said second cryptographic unit is of the form $K = (\alpha^x)^b(p_a)^y$.
37. The method according to any one of claims 27 to 36 wherein said information made public by one of said second correspondent B and said first correspondent A is information made public by said second correspondent.
38. The method according to any one of claims 27 to 37 wherein said method includes operations based on an underlying elliptic curve group.
39. A correspondent configured to permit exchange of information with another correspondent, said correspondent having a cryptographic unit, a private key and a public key derived from a generator and said private key, said correspondent further configured to perform the method of any one of claims 15 to 38.
40. A method for transporting a key between a first correspondent A and a second correspondent B to permit exchange of information therebetween, said first correspondent A having a first cryptographic unit, a private key a , and a public key p_a derived from a generator α and said private key a , and a second correspondent B having a second cryptographic unit, a private key b , and a public key p_b derived from said generator α and said private key b , said method comprising:

- i) said first cryptographic unit selecting a first random integer x and a second random integer t ;
- ii) said first cryptographic unit operating upon said first random integer x , said second random integer t , said public key p_b and said generator α to derive a first component r ;
- iii) said first cryptographic unit operating on said first component r , said first random integer x , and said private key a to derive a second component s ;
- iv) said first cryptographic unit computing a session key K using information private to said first correspondent;
- v) said first cryptographic unit generating a value h of a function $F[\pi, K]$ to thereby bind the values of π and K , wherein $F[\pi, K]$ denotes a cryptographic function applied to π and K , and wherein π is obtained from information made public by one of said first correspondent A and said second correspondent B;
- vi) said first cryptographic unit forwarding to said second cryptographic unit a message including said first component r , said second component s , and said value h ;
- vii) said second cryptographic unit constructing a corresponding session key K' from information made public by said first correspondent A and from information that is private to said second correspondent B;
- viii) said second cryptographic unit generating a corresponding value h' of a function $F[\pi, K']$ wherein $F[\pi, K']$ denotes a corresponding cryptographic function applied to π and K' to thereby bind the values of π and K' ; and
- ix) said second cryptographic unit comparing said corresponding value h' to said value h to confirm their correspondence.

41. The method according to claim 40 wherein said message includes an identification of said first correspondent A.

42. The method according to claim 40 or claim 41 wherein said cryptographic function $F[\pi, K]$ is a cryptographic hash of π and K , and said corresponding cryptographic function $F[\pi, K']$ is a cryptographic hash of π and K' .
43. The method according to any one of claim 40 to 42 wherein said first component r is of the form $r = (p_b)^t \alpha^{-x}$.
44. The method according to any one of claims 40 to 43 wherein said second component s is of the form $s = x - ra$.
45. The method according to any one of claims 40 to 44 wherein said session key K is computed using said second random integer t and said generator α .
46. The method according to any one of claims 40 to 45 wherein said session key K is of the form $K = \alpha^t$.
47. The method according to any one of claims 40 to 46 wherein said corresponding session key K' is of the form $K' = (r\alpha^x)^{b^{-1}}$.
48. The method according to any one of claims 40 to 47 wherein said information made public by one of said second correspondent B and said first correspondent A is information made public by said first correspondent A.
49. The method according to any one of claims 40 to 48 wherein said method includes operations based on an underlying elliptic curve group.
50. A method for transporting a key between a first correspondent A and a second correspondent B to permit exchange of information therebetween, said first correspondent A having a cryptographic unit, a private key a , and a public key p_a derived from a generator α and said private key a , said method comprising:
- i) said cryptographic unit selecting a first random integer x and a second random integer t ,

- ii) said cryptographic unit operating upon said first random integer x , said second random integer t , a public key p_b of said second correspondent B, and said generator α to derive a first component r ,
- iii) said cryptographic unit operating on said first component r , said first random integer x , and said private key a to derive a second component s ;
- iv) said cryptographic unit computing a session key K using information private to said first correspondent; a corresponding session key K' being computable by said second correspondent B from information made public by said first correspondent A and from information that is private to said second correspondent B;
- v) said cryptographic unit generating a value h of a function $F[\pi, K]$ to thereby bind the values of π and K , wherein $F[\pi, K]$ denotes a cryptographic function applied to π and K , and wherein π is obtained from information made public by one of said first correspondent A and said second correspondent B; and
- vi) said cryptographic unit forwarding to said second cryptographic unit a message including said first component r , said second component s , and said value h ; whereby said second correspondent B is able to generate a corresponding value h' of a function $F[\pi, K']$ and compare said corresponding value h' to said value h to confirm their correspondence.

51. The method according to claim 50 wherein said message includes an identification of said first correspondent A.

52. The method according to claim 50 or claim 51 wherein said cryptographic function $F[\pi, K]$ is a cryptographic hash of π and K .

53. The method according to any one of claim 50 to 52 wherein said first component r is of the form $r = (p_b)^t \alpha^{-x}$.

54. The method according to any one of claims 50 to 53 wherein said second component s is of the form $s = x - ra$.

55. The method according to any one of claims 50 to 54 wherein said session key K is computed using said second random integer t and said generator α .

56. The method according to any one of claims 50 to 55 wherein said session key K is of the form $K = \alpha'$.

57. The method according to any one of claims 50 to 56 wherein said information made public by one of said second correspondent B and said first correspondent A is information made public by said first correspondent A.

58. The method according to any one of claims 50 to 57 wherein said method includes operations based on an underlying elliptic curve group.

59. A method for transporting a key between a first correspondent A and a second correspondent B to permit exchange of information therebetween, said second correspondent B having a cryptographic unit, a private key b , and a public key p_b derived from said generator α and said private key b , said method comprising:

i) said cryptographic unit receiving a message including a first component r , a second component s , and a value h ; said first component r having been generated by said first correspondent A by operating upon a first random integer x , a second random integer t , said public key p_b , and said generator α ; said second component s having been generated by said first correspondent A by operating upon said first component r , said first random integer x , and a private key a of said first correspondent A; and said value h having been generated by said first correspondent A by applying a cryptographic function $F[\pi, K]$ to bind values π and K , wherein K is a session key that was computed by the first correspondent A using information private to said first correspondent A, and π is obtained from information made public by one of said first correspondent A and said second correspondent B;

ii) said cryptographic unit constructing a corresponding session key K' from information made public by said first correspondent A and from information that is private to said second correspondent B;

iii) said cryptographic unit generating a corresponding value h' of a function $F[\pi, K']$, wherein $F[\pi, K']$ denotes a corresponding cryptographic function applied to π and K' to thereby bind the values of π and K' ; and

iv) said cryptographic unit comparing said corresponding value h' to said value h to confirm their correspondence.

60. The method according to claim 59 wherein said message includes an identification of said first correspondent A.

61. The method according to claim 59 or claim 60 wherein said cryptographic function $F[\pi, K]$ is a cryptographic hash of π and K , and said corresponding cryptographic function $F[\pi, K']$ is a cryptographic hash of π and K' .

62. The method according to any one of claim 59 to 61 wherein said first component r is of the form $r = (p_b)^t \alpha^{-x}$.

63. The method according to any one of claims 59 to 62 wherein said second component s is of the form $s = x - ra$.

64. The method according to any one of claims 59 to 63 wherein said corresponding session key K' is of the form $K' = (r\alpha^x)^{b^{-1}}$.

65. The method according to any one of claims 59 to 64 wherein said information made public by one of said second correspondent B and said first correspondent A is information made public by said first correspondent A.

66. The method according to any one of claims 59 to 65 wherein said method includes operations based on an underlying elliptic curve group.

67. A system comprising a first correspondent A and a second correspondent B, said first correspondent A and said correspondent B configured to permit exchange of information therebetween, said first correspondent A having a first cryptographic unit, a first private key, and a first public key derived from a generator and said first private key, said second correspondent B having a second cryptographic unit, a second private key, and a second public key derived from said generator and said second private key, both said first

correspondent A and said second correspondent B further configured to perform the method of any one of claims 40 to 49.

68. A correspondent configured to permit exchange of information with another correspondent, said correspondent having a cryptographic unit, a private key and a public key derived from a generator and said private key, said correspondent further configured to perform the method of any one of claims 50 to 66.

22059555.2

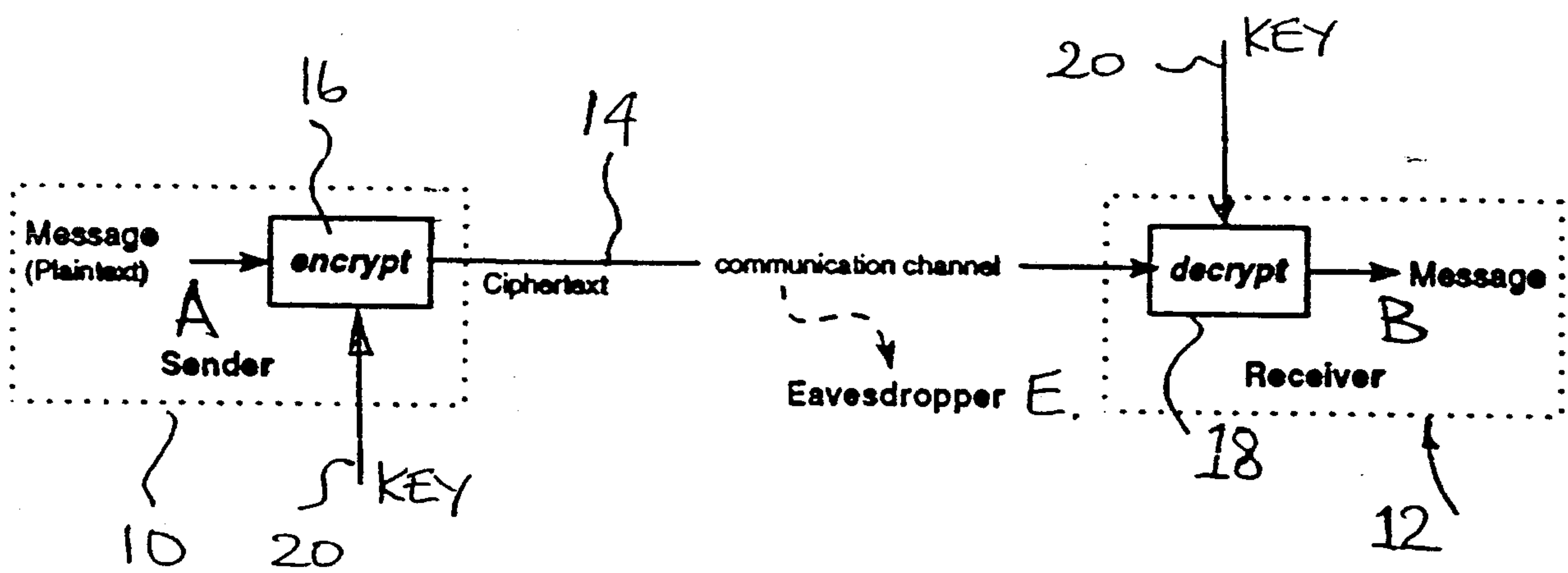


Fig. 1

