Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2550362 C 2015/12/01

(11)(21) **2 550 362**

(12) BREVET CANADIEN / CANADIAN PATENT

(13) **C**

(22) **Date de dépôt/Filing Date:** 2006/06/14

(41) **Mise à la disp. pub./Open to Public Insp.:** 2006/12/14

(45) **Date de délivrance/Issue Date:** 2015/12/01

(30) **Priorité/Priority:** 2005/06/14 (US60/690,156)

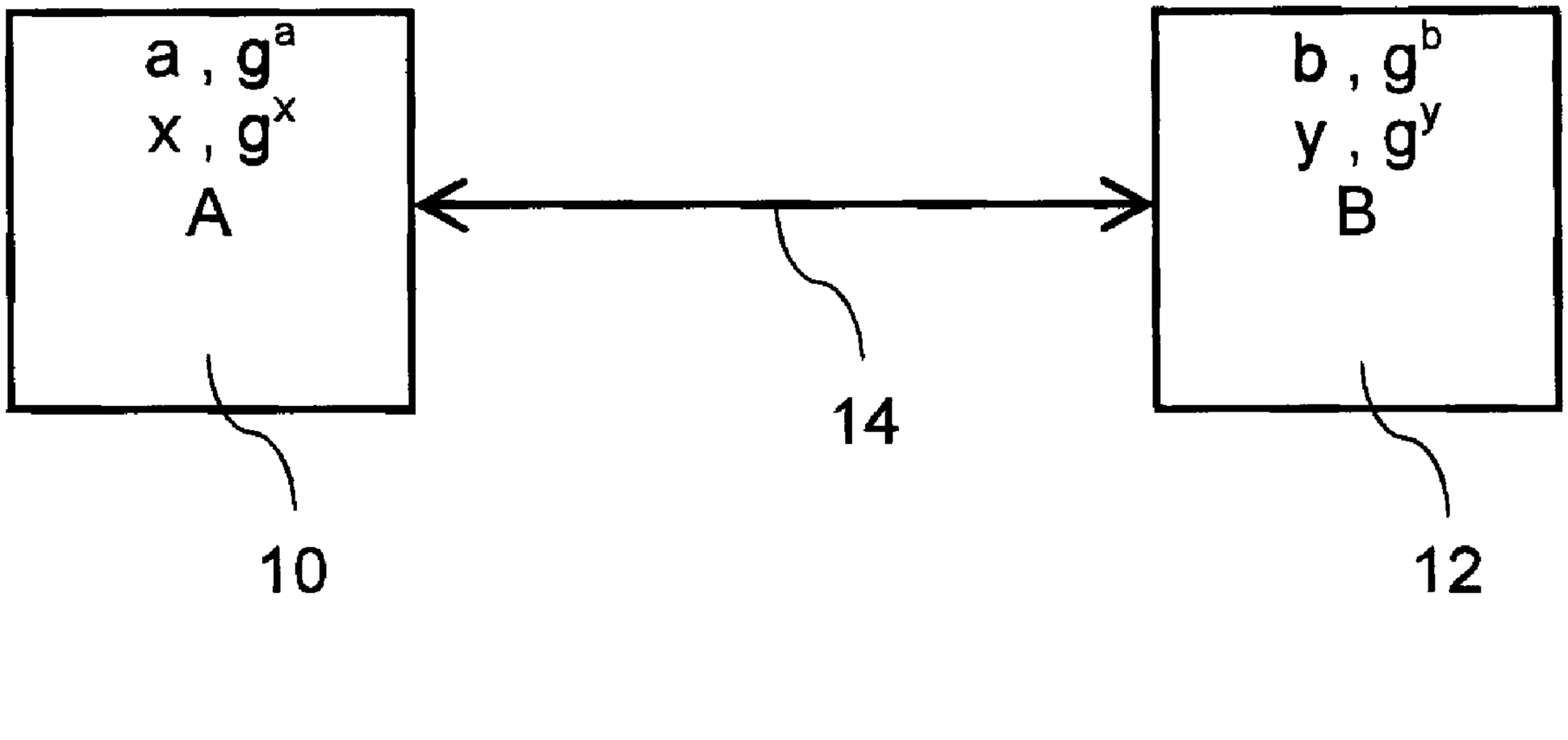
(51) **Cl.Int./Int.Cl.** ***H04L 9/30*** (2006.01),
H04L 9/14 (2006.01)

(72) **Inventeur/Inventor:**
MENEZES, ALFRED, CA

(73) **Propriétaire/Owner:**
CERTICOM CORP., CA

(74) **Agent:** ROWAND LLP

(54) **Titre : PROTOCOLE AMELIORE DE MISE EN ACCORD ET DE TRANSMISSION DE CLE**
(54) **Title: ENHANCED KEY AGREEMENT AND TRANSPORT PROTOCOL**



(57) **Abrégé/Abstract:**
A key agreement protocol for use in a public key cryptographic scheme between a pair of correspondents each of which has a long term public key and an ephemeral public key. The protocol includes the steps of exchanging the ephemeral public keys between the correspondents for computing a shared secret at each correspondent and utilizing the shared secret to obtain a common key, wherein the validity of the ephemeral public keys is checked by the recipient thereof prior to use of the common key.

ABSTRACT

A key agreement protocol for use in a public key cryptographic scheme between a pair of correspondents each of which has a long term public key and an ephemeral public key. The protocol includes the steps of exchanging the ephemeral public keys between the correspondents for computing a shared secret at each correspondent and utilizing the shared secret to obtain a common key, wherein the validity of the ephemeral public keys is checked by the recipient thereof prior to use of the common key.

Enhanced Key Agreement and Transport Protocol

FIELD OF THE INVENTION

[0001] The present invention relates to data transmission systems and in particular systems for implementing key transportation and key agreement protocols within a public key infrastructure.

BACKGROUND OF THE INVENTION

[0002] Various protocols exist for establishing common keys between a pair of entities connected within a data communication system or for transporting keys between such entities. Many of theses protocols are based upon the fundamental Diffie-Hellman protocol in which a piece of information private to one of the correspondents is combined with public information from the other correspondent to arrive at a common key. The protocol known as the MQV protocol after the inventors Menezes, Qu and Vanstone and exemplified in the PCT application WO 98/18234, is recognized as one of the most efficient of known authenticated Diffie-Hellman protocols that use public key authentication. It is recognized as offering superior performance whilst inherently possessing excellent security properties. As a result, MQV has been widely standardized and has recently been chosen by the NSA as the key exchange mechanism underlying the next generation of cryptography to protect the United States government information.

[0003] Proposals have been made to modify the MQV protocol to implement a variation of the protocol. Whilst these proposals have been made to address what are perceived as potential flaws in the underlying MQV concept, further examination has shown that such flaws do not exist and that the proposed modifications, contrary to the assumptions made by the proponents, themselves introduce additional security risks.

[0004] It is therefore an object of the present invention to obviate or mitigate the above disadvantages.

[0005] In general terms, the present invention provides a key agreement protocol in which a signature component of one correspondent includes a hash of the public key of the one

correspondent and the identity of the intended recipient. During the exchange of information, the validity of at least one of the public keys used in the exchange is determined. The resultant shared key may also be checked for its validity.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] An embodiment of the invention will now be described by way of example only with the reference to accompanying drawings in which:

[0007] Figure 1 is a schematic representation of a data communication system.

[0008] Figure 2 is a flow chart showing the exchange of information between correspondents in the data communication system.

DETAILED DESCRIPTION OF THE INVENTION

[0009] Referring therefore to Figure 1 a pair of correspondents 10, 12 exchange information over a data communication link 14. Each of the correspondents implement a cryptographic protocol in a cryptographic unit 16, 18 embedded within the respective correspondents. The cryptographic protocol is a public key protocol key implemented over a finite field. Such protocols use the intractability of the discrete log problem to secure a private key even where the corresponding public is known. A particularly useful protocol is that based on the properties of an elliptic curve defined over a finite field.

[0010] An elliptic curve E is a set of points that satisfy the equation $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$. The elements of a finite field that satisfy the equation of an elliptic curve, together with the point at infinity, define an elliptic curve group G. The group G may have subgroups S and the group G, or each subgroup S, as the case may be, has a generator g that will generate each element of the group or subgroup. The number of points in the group or subgroup is the order q of the group or subgroup. Certain types of curves will have a cofactor h, as explained more fully at page 114 of Guide to Elliptic curve Cryptography published by Springer under ISBN 0-387-95273-X. The domain parameters including underlying field F, the

curve E, the group G or subgroup S and the generator g are all parameters of the protocol that are publically known.

[0011] Each of the correspondents 10, 12 have respective long term private keys a, b and corresponding public keys g^a, g^b respectively. Each of the cryptographic unites 16, 18, of the correspondents 10, 12 is also capable of generating a random integer x, y respectively and computing a corresponding ephemeral or session public key g^x, g^y respectively. The long term public keys g^a, g^b are initially presented to a certifying authority, CA, who determines that they satisfy certain arithmetic properties to ensure that they may validly be used as public keys. In particular, the CA establishes that the long term public keys do not belong to a small group or subgroup of less than a predetermined order, referred to as a small subgroup check, and that the keys represent points on the curve E. By performing the substitution of an unsuitable key by an interloper to gain access to secret information is avoided.

[0012] As a first exchange in a session between the correspondents 10, 12, correspondent 10 forwards a message consisting of the identity of correspondent 10, A, and the ephemeral public key g^x. Similarly, the correspondent 12 forwards the message including the identity of correspondent 12, B and the ephemeral public key g^y.

[0013] Upon receipt of the ephemeral public keys, each correspondent 10, 12 utilizes the cryptographic unit 16, 18, to perform a public key validation within the correspondent to again check for the suitability of the received ephemeral public key. The validation again requires checking the point is on the curve E and that it is not part of a small subgroup. The small subgroup check may be performed for particular types of curve by exponentiating the key by the cofactor h and checking that the result does not correspond to the point at infinity.

[0014] Each of the correspondents then computes a signature component s_A and s_B of the form $s_A = x + aH(g^x, B)$ and $s_B = y + bH(g^y, A)$, where H is a cryptographically secure hash function.

[0015] A common shared secret is then computed at each correspondent with the correspondent 10 computing $k = \left[\left(g^y \left(g^b\right)^{H\left(g^x, A\right)}\right)\right]^{s_A}$ and the correspondent 12 computing $k = \left[\left(g^x\right)\left(g^a\right)^{H\left(g^y, B\right)}\right]^{s_B}$.

[0016] Finally, the secret key K is obtained by applying a suitable key derivation function F (for example a cryptographic hash function) to the shared secret k: K=F(k). The secret key K is computed by each of the correspondent and should be the same to permit exchange of further messages in a secure manner by utilisation of the common key K.

[0017] By performing public key validation on each of the public keys utilised, malicious attacks on the protocol may be thwarted and the integrity of the data exchange may be assured.

[0018] If an elliptic curve group is used for which the cofactor h is small, then public key validation of the exchanged public keys g^x and g^y can be sped up by omitting the expensive exponentiation associated with the small subgroup check that guarantees that the key K is in the main group of order q. Instead, the recipient simply checks that the received public key g^x, g^y is a point on the curve (but not necessarily one in the group of order q). Then, the shared secret k is raised to the power of the (small) cofactor h, and the result is checked to ensure that it does not correspond to the point at infinity. This modified shared secret is then hashed to yield the secret key K.

[0019] In an alternative embodiment, validation of the shared secret key K is computed by an exponent of either s_A mod q or s_B mod q where q is the order of the group G. Thus correspondent 10 computes $k = \left[\left(g^y \left(g^b\right)^{H\left(g^x, A\right)}\right)\right]^{s_A \bmod q}$ and correspondent 12 computes $k = \left[\left(g^x\right)\left(g^a\right)^{H\left(g^y, B\right)}\right]^{s_B \bmod q}$. By reducing the exponent mod q, the bit length of the exponent is reduced and accordingly the computational efficiency increased. The shared secret K may then be checked for conformance with the required mathematical properties, e.g. by checking $k \neq \infty$ and then used to compute the shared key K.

IN THE CLAIMS

1. A method of establishing a common key used by a correspondent in a public key cryptographic scheme with another correspondent, the public key cryptographic scheme utilizing a finite group G, each of the correspondents having a respective long term public key, a respective ephemeral public key, and respective identity information associated therewith, the method comprising:

the correspondent forwarding a correspondent ephemeral public key and correspondent identity information over a data communication link to the other correspondent;

the correspondent receiving an other correspondent ephemeral public key and an other correspondent identity information over the data communication link from the other correspondent;

the correspondent checking a validity of the received ephemeral public key within the correspondent to confirm that the received ephemeral public key is a member of the finite group G that satisfies pre-selected criteria for use as a valid public key;

the correspondent applying a cryptographic operation to compute a shared secret using the forwarded ephemeral key, the received ephemeral key, the forwarded identity information and the received identify information; and,

the correspondent utilizing the shared secret to obtain the common key.

2. The method according to claim 1, wherein the pre-selected criteria comprises checking that the received ephemeral public key is not a member of a sub group of less than a predetermined number of elements.

3. The method according to claim 1, wherein the cryptographic scheme is an elliptic curve cryptosystem utilizing a defined elliptic curve and the correspondent confirms that the received ephemeral public key is a point on the defined elliptic curve.

4. The method according to claim 1 further comprising:

the correspondent receiving an other correspondent long term public key over the data communication link from the other correspondent; and,

the correspondent checking a validity of the received long term public key within the correspondent to confirm that the received long term public key is a member of the finite group G that satisfies pre-selected criteria for use as a valid public key;

wherein the correspondent applying the cryptographic operation to compute the shared secret further utilizes the received long term public key.

5. The method according to claim 1, wherein the correspondent applies the cryptographic operation to compute a signature component to bind the received identity information, a long term private key, and the long term public key of the correspondent.

6. The method according to claim 5 wherein the shared secret is computed by exponentiating the received long term public key and the received ephemeral public key with the signature component.

7. The method according to claim 6 wherein the signature component is reduced mod q where q is the order of the group utilized in the cryptographic scheme.

8. The method according to claim 6 wherein the shared secret is exponentiated by the cofactor of the elliptic curve group and a result compared to the point at infinity to validate the received ephemeral public key.

9. The method according to claim 1, further comprising the step of validating the shared secret prior to using the common key.

10. A communication device configured for communicating with another correspondent communication device over a data communication link, the communication device having a cryptographic unit, the cryptographic unit being configured to implement a method of establishing a common key shared with the other correspondent communication device in a public key cryptographic scheme, the public key cryptographic scheme utilizing a finite group G, each of the communication devices having a respective long term public key, a respective ephemeral public key, and respective identity information associated therewith, the

cryptographic unit operative to:

forward a correspondent ephemeral public key and correspondent identity information over a data communication link to the other correspondent;

receive an other correspondent ephemeral public key and an other correspondent identity information over the data communication link from the other correspondent;

check a validity of the received ephemeral public key within the correspondent to confirm that the received ephemeral public key is a member of the finite group G that satisfies pre-selected criteria for use as a valid public key;

apply a cryptographic operation to compute a shared secret using the forwarded ephemeral key, the received ephemeral key, the forwarded identity information and the received identify information; and,

utilize the shared secret to obtain the common key.

11. The communication device according to claim 10, wherein the pre-selected criteria comprises checking that the received ephemeral public key is not a member of a sub group of less than a predetermined number of elements.

12. The communication device according to claim 10, wherein the cryptographic scheme is an elliptic curve cryptosystem utilizing a defined elliptic curve and the correspondent is operative to check the validity by checking that the received ephemeral public key is a point on the defined elliptic curve.

13. The communication device according to claim 10 further operative to:

receive an other correspondent long term public key over the data communication link from the other correspondent; and,

to check a validity of the received long term public key within the correspondent to confirm that the received long term public key is a member of the finite group G that satisfies pre-selected criteria for use as a valid public key;

wherein the correspondent is operative to apply the cryptographic operation utilizing the received long term public key.

14. The communication device according to claim 10, wherein the computing device is operative to apply the cryptographic operation to bind the received identity information, a long term private key, and the long term public key of the correspondent.

15. The communication device according to claim 14 wherein the computing device is operative to compute the shared secret by exponentiating the received long term public key and the received ephemeral public key with a signature component computed by the cryptographic operation.

16. The communication device according to claim 15 wherein the computing device is operative to reduce the signature component mod q where q is the order of the group utilized in the cryptographic scheme.

17. The communication device according to claim 15 wherein the computing device is operative to exponentiate the shared secret by the cofactor of the elliptic curve group and to compare a result to the point at infinity to validate the received ephemeral public key.

18. The communication device according to claim 10, wherein the computing device is further operative to validate the shared secret prior to using the common key.

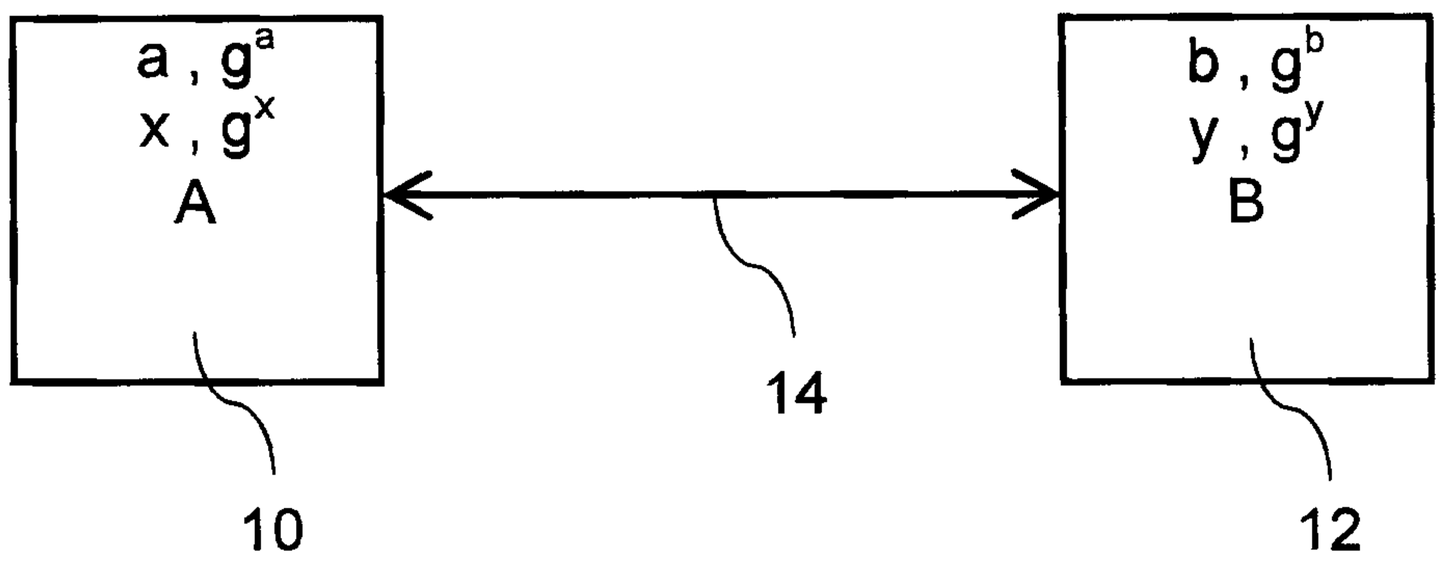


FIG 1

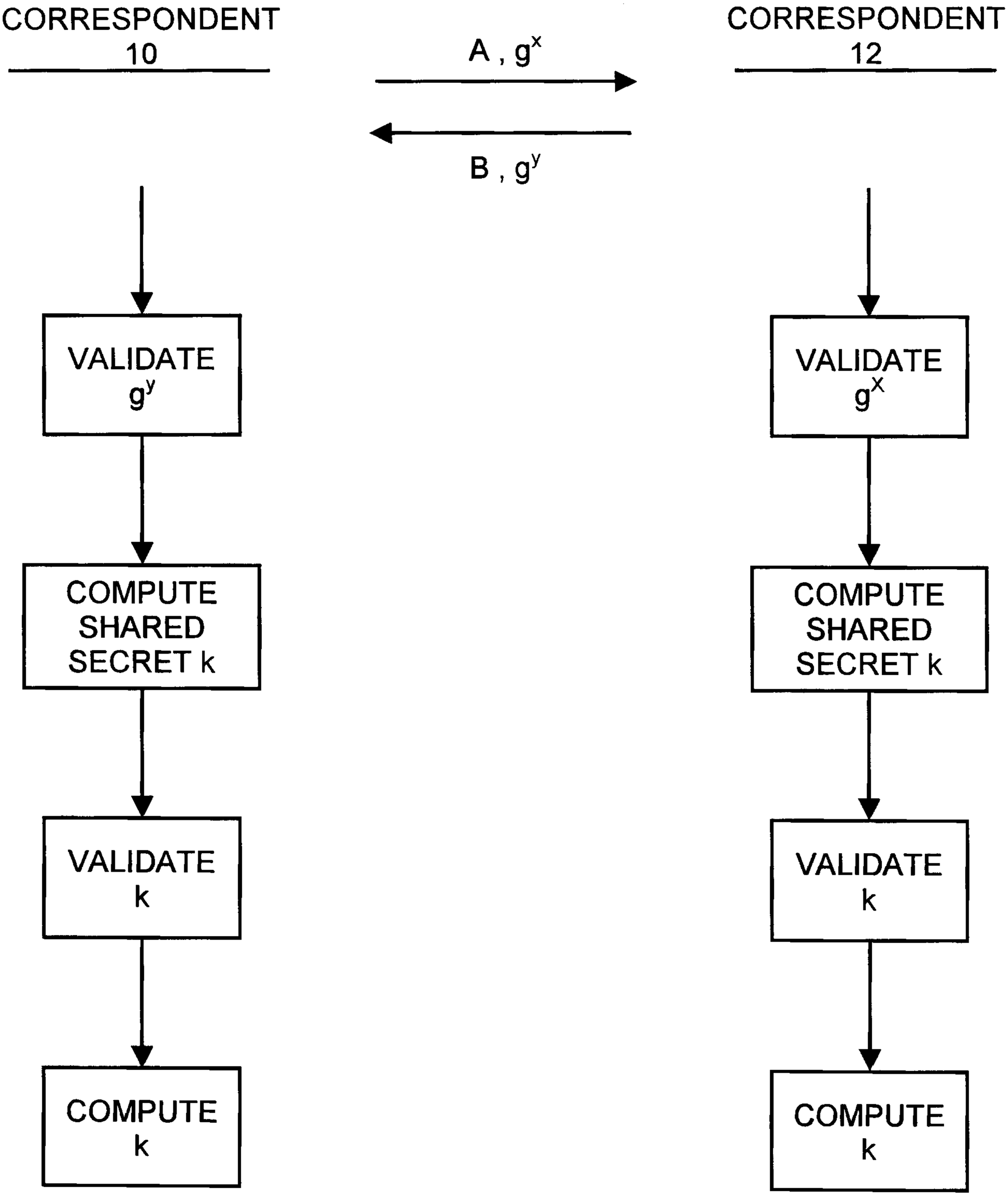
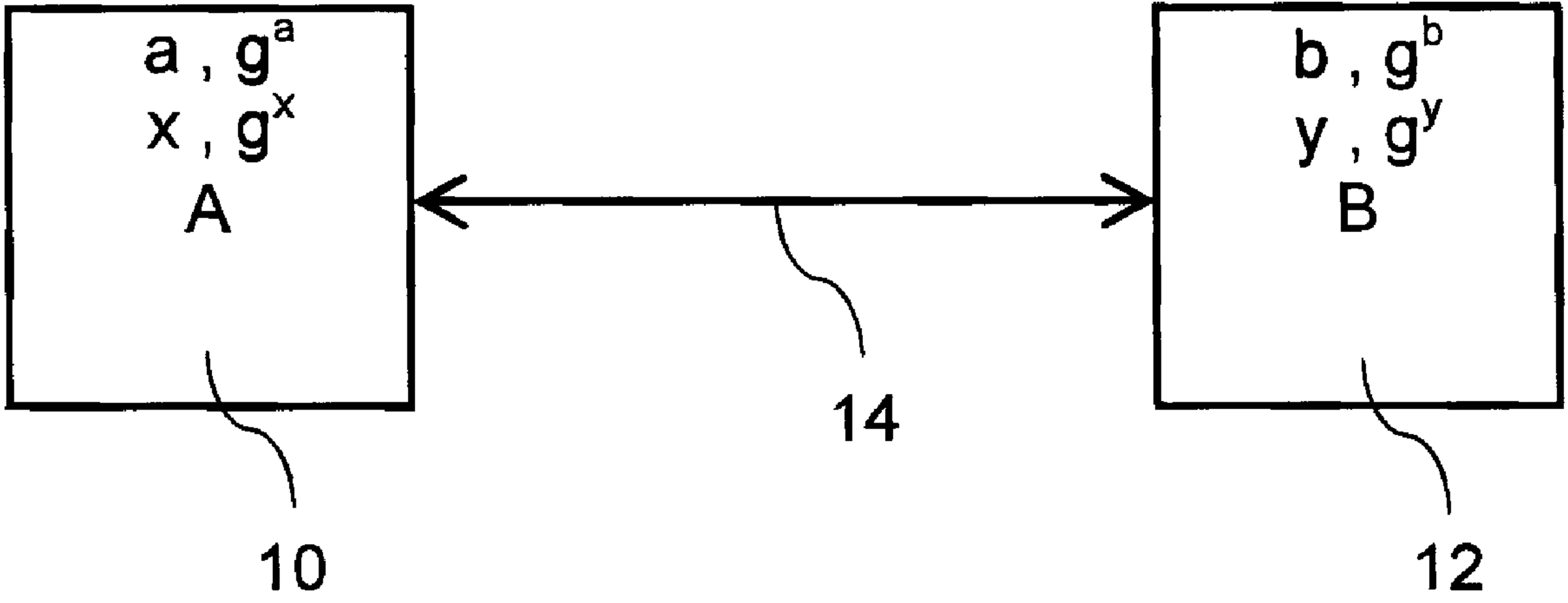

CORRESPONDENT
10
A , g^x
CORRESPONDENT
12
B , g^y
VALIDATE
g^y
VALIDATE
g^X
COMPUTE
SHARED
SECRET k
COMPUTE
SHARED
SECRET k
VALIDATE
k
VALIDATE
k
COMPUTE
k
COMPUTE
k

FIG 2


a , g^a
x , g^x
A
b , g^b
y , g^y
B
14
10
12