DESCRIPTION

MEMBER CERTIFICATE ACQUIRING DEVICE, MEMBER CERTIFICATE ISSUING DEVICE, GROUP SIGNING DEVICE, AND GROUP SIGNATURE VERIFYING DEVICE

Technical Field

[0001]

The present invention relates to a group signing system which creates and verifies a signature for certifying that a member belonging to a group is a member of the group, and particularly to a group signing system which utilizes bilinear mapping.

Background Art

[0002]

Related art of group signature which use bilinear mapping includes a group signature described in Dan Boneh, Xavier Boyen: "Short Group Signature,: Advances in Cryptology -- CRYPTO 2004," Lecture Notes in Computer Science 3152, pp. 41-55, 2004, Springer. The outline of this group signature will be described below.

[0003]

Let a randomly selected unknown γ of a field Z/pZ with p being a prime number be the group secret key.

[0004]

Let a letter string which describes: the prime number p; group 1, group 2 and group T which are of order number p; a bilinear map e from group 1 and group 2 to group T; an isomorphic map ϕ from group 2 to group 1; and a hash

function Hash for mapping a letter string to field (Z/pZ), a generator G_2 of group 2, a generator G_1 of group 1 where $\phi(G_2 = G_1$, a randomly selected unknown H of group 1, and $W = [\gamma]G_2$ be the group public key.

[0005]

Where, W is the point of γ times G_2.

[0006]

Further, let randomly selected two points ξ_1, ξ_2 on field Z/pZ be the tracking secret key.

[0007]

Let randomly selected two points on group 2 in which $[\xi_1]U = [\xi_2]V = H$ be the tracking public key. And let a randomly selected point x on field Z/pZ be the member secret key.

[0008]

Further, Let a randomly selected point y on field Z/pZ and A where $A = [1/(\gamma+y)]([1-x]G_1)$be the member certificate.

[0009]

Hereinafter, the group signing device will be described.

[0010]

The group signing device is input with a message to be signed, a group public key, a tracking public key, a member secret key, a member certificate, and a random number.

[0011]

The group signing device randomly selects points α and β on Z/pZ using an input random number and generates encrypted text, $T_1 = [\alpha]U$, $T_2 = [\beta]V$, $T_3 = [\alpha+\beta]H$.

[0012]

The group signing device further randomly selects points α', β', δ'_1, δ'_2, and y' on Z/pZ using an input random number, and generates a commitment, $R_1 = [\alpha']U$, $R_2 = [\beta']V$, $R_3 = e(T_3,G_2)^{(x')} \cdot e(H,W)^{(-\alpha'-\beta')} \cdot e(H,G_2)^{(-\delta'_1-\delta'_2)} \cdot e(H,G_2)^{(y')}$, $R_4 = [x']T_1 - [¥delta'_1]U$, $R_5 = [x']T_2 - [¥delta'_2]V$, where symbol [^] means a power modulo operation.

[0013]

The group signing device generates a hash value of a group public key, a tracking public key, a message, and $U,V,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5$ to use as challenge value c.

[0014]

The group signing device generates a response, $s\alpha = \alpha' + c\alpha$, $s\beta = \beta' + c\beta$, $s_x = x' + cx$, $s\delta_1 = \delta'_1 + cx\alpha$, $s\delta_2 = \delta'_2 + cx\beta$, $s_y = y' + xy$.

[0015]

The group signature outputs $T_1,T_2,T_3,c,s\alpha,s\beta,s_x,s\delta_1,s\delta_2,s_y$ as the group signature for message m.

[0016]

Hereinafter, the group-signature verifying device will be described.

[0017]

The group-signature verifying device is input with a signed message, a group public key, and a tracking public key.

[0018]

The group-signature verifying device generates $R_1 = [s\alpha]U - [c]T_1$, $R_2 = [s\beta]V - [c]T_2$, $R_3 = e(T_3,G_2)^{(s_x)} \cdot e(H,W)^{(-s\alpha-s\beta)} \cdot e(H,G_2)^{(-s\delta_1-s\delta_2)} \cdot e(H,G_2)^{(s_y)} (e(G_1,G_2)/e(T_3,W))^{(c)}$, $R_4 = [s_x]T_1 - [s\delta_1]U$, $R_5 = [s_x]T_2 - [s\delta_2]U$, and generates a hash value of the group public key, the tracking public key, the signed message and $U,V,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5$ to verify if this corresponds to

challenge value c. If there is a correspondence, it is judged that the group signature is valid and, if not, invalid.

Disclosure of the Invention

[0019]

A first problem in the above described related art is that the security of the encrypted text used in the group signature relies on the assumption that it is difficult to solve the linear Diffie-Hellman discrimination problem. Therefore, the security of the entire group signing system also relies on this assumption. This assumption has been firstly proposed in the above mentioned reference to demonstrate the security of the proposed group signature, and few have attempted to solve this problem. Therefore, it is highly likely that a solution will be found in the near future, and thus the above mentioned proposed group signature may not provide sufficient security.

[0020]

A second problem is that the security of the encrypted text used in the group signature relies on a generic group mode as well as on the assumption that it is difficult to solve the linear Diffie-Hellman discrimination problem. The security of a scheme in which security is provided by this general group is based on nothing more than a prediction, so that even in cases where security is provided by the general group model, in reality, dangerous encryption schemes may still occur. Therefore, it is likely that a solution will be proposed in the near future, and the proposed group signature may not provide sufficient security.

[0021]

A third problem is that there are large amount of calculation and signature data. In order to make the group signature easier to use, it is desirable to reduce the amount of calculation and signature data.

[0022]

The member-certificate acquiring device of the present invention, which is input with a group public key and a random number, and outputs a member certificate and a member secret key by communicating with a member-certificate issuing device, is characterized in that when input with the group public key which includes: a description for four groups: group 1, group 2, group T, and group E, of the same order number; a description of bilinear mapping from group 1 and group 2 to group T; each generator of group 1, group 2, group T, and group E; and a signature public key of a signature scheme using the group 1, the group 2, and the group T, the member-certificate acquiring device sends to the member secret key including an integer not larger than the order number; member evidence which is a value given by multiplying the generator of the Group E by the member secret key; and an element of the group 1, group 2, which is a value given by multiplying the generator of group 1 or group 2 by the member secret key, and thereafter upon receipt of a signature for the member secret key, which is verifiable by the signature public key, from the member certificate issuing device, uses the signature as the member certificate.

[0023]

The member-certificate issuing device of the present invention, which is input with a group public key, a group secret key and a random number and which outputs a member evidence for use in identifying a member by communicating with a member-certificate acquiring device, is characterized in that the member-certificate issuing device is input with the group public key

which includes: a description for four groups: group 1, group 2, group T, and group E, of the same order number; a description of bilinear mapping from group 1 and group 2 to group T; each generator of group 1, group 2, group T, and group E; and a signature public key of a signature scheme using group 1, group 2, and group T, and the group secret key which includes a signature secret key corresponding to the signature public key of a signature scheme using group 1, group 2, and group T, and upon receipt of a member evidence which is a value given by multiplying the generator of the group E by the member secret key, and an element of group 1 or group 2 which is a value given by multiplying the generator of group 1 or group 2 by the member secret key from the member-certificate acquiring device, generates a signature for the member secret key using the signature secret key to send the signature to the member-certificate acquiring device as the member certificate.

[0024]

The group signing device of the present invention is a group signing device, which is input with a group public key, a tracking public key, a member certificate, a member secret key, and a message and outputs a group signature for the message, characterized in that the group signing device comprises an encryption device for creating an encrypted text in which part of the member evidence generated from the member secret key is encrypted by a tracking public key from: the group public key including a description for four groups: group 1, group 2, group T, and group E, of the same order number, a description of bilinear mapping from group 1 and group 2 to group T, each generator of group 1, group 2, group T, and group E, a signature public key of a signature scheme utilizing group 1, group 2, and group T; the tracking public key comprising an element of the group E; and the member secret key.

[0025]

In the above described case, the group signing device may comprise a knowledge-proof-statement generating device which generates a knowledge proof statement which is data for proving that a secret key encrypted into the encrypted text and a signature for the aforementioned secret key can be calculated from input data, and the group signature to be output may include a knowledge proof statement by the knowledge-proof-statement generating device.

[0026]

Further, the above described knowledge-proof-statement generating device may comprise:

a commitment generating device, which is input with the group public key, the tracking public key, the member secret key, the member certificate, and the random number, and generates a commitment to encryption which is data for proving knowledge of a random number for encryption, and a commitment to member certificate which is data for proving knowledge of signature and member secret key, to output the commitment to encryption and the commitment to member certificate as a commitment;

a challenge-value generating device which is input with the group public key, the tracking public key, the encrypted text, and the commitment and which outputs a hash value of the foregoing values as a challenge value; and

a response generating device which is input with the group public key, the member secret key, the member certificate, the random number, and the challenge value and which outputs a response of encryption and a response of member certification as a response.

[0027]

Furthermore, the above described group signature may comprise the above described encrypted text, the above described commitment, and the above described response.

[0028]

Furthermore, the above described group signature may comprise the above described encrypted text, the above described challenge value, and the above described response.

[0029]

The group-signature verifying device of the present invention into which is input with a group public key, a tracking public key, a message and a group signature, when input with a group public key which includes a description for four groups: group 1, group 2, group T, and group E, of the same order number, a description of bilinear mapping from group 1 and group 2 to group T, each generator of group 1, group 2, group T, and group E, and a signature public key of the signature scheme using the group 1, the group 2, and the group T; a tracking public key comprising an element of the group E; and a group signature including an encrypted text in which part of member evidence generated by a member secret key is encrypted by a tracking public key, judges if the above described group signature is a valid group signature for the message to output "valid" or "invalid."

[0030]

In the above described case, the group-signature verifying device may comprise a knowledge-proof-statement verifying device which verifies that a knowledge proof statement is data to prove that a secret key which is used to generate part of member evidence encrypted into the above described encrypted text, and a signature for the secret key can be calculated from data

input into the group signing device and from data included in the group signing device, and

the above group signature may include a knowledge proof statement which has been verified by the proof-statement verifying device.

[0031]

Moreover, the group signature may comprise the above described encrypted text, the above described commitment, and the above described response; and

the above described knowledge-proof-statement verifying device may comprise:

a challenge-value generating device which is input with the above described group public key, the above described tracking public key, the above described encrypted text, and the above described commitment, and outputs a hash value of the foregoing values as a challenge value; and

a response verifying device which is input with the above described group public key, the above described tracking public key, the above described encrypted text, the above described commitment, the above described challenge value, and the above described response and outputs "valid" or "invalid" depending on whether or not these inputs satisfy a given equation, wherein the output of the response verifying device may be output as the output of the group-signature verifying device.

[0032]

Moreover, the above described group signature may comprise the above described encrypted text, the above described challenge value, and the above described response, and

the above described knowledge-proof-statement verifying device comprises:

a commitment generating device which is input with the above described group public key, the above described tracking public key, the above described response, and the above described challenge value, and outputs a commitment to encryption and a commitment to member certificate as a commitment; and

a response verifying device which is input with the above described group public key, the above described tracking public key, the above described encrypted text, and the above described commitment, and outputs "valid" or "invalid" depending on whether or not a hash value of the foregoing values corresponds to the above described challenge value; wherein

the output of the above described response verifying device may be output as the output of the group-signature verifying device.

[0033]

The tracking device of the present invention is input with a group public key, a tracking public key, a group signature, and a tracking secret key, and decrypts the encrypted text of part of the member evidence generated from a member secret key contained in the group signature to output the part of member evidence which is a value uniquely determined from the member secret key.

[0034]

The group signing system of the present invention, which comprises the above described member-certificate acquiring device, a member-certificate issuing device, a group signing device, a group-signature verifying device, and a tracking device, is characterized in that

the above described member-certificate acquiring device, which communicates with the above described member-certificate issuing device to acquire a member certificate and a member secret key; inputs the acquired member certificate, the acquired member secret key, a message, a group

public key, and a tracking public key into the above described group signing device to acquire a group signature for the above described message; and inputs the above described message and the acquired group signature into the above described group-signature verifying device to verify that the acquired group signature is a valid group signature for the above described message and to input the above described group signature into the above described tracking device thereby outputting a member evidence representing the member which has generated the group signature.

[0035]

In order to solve the first problem, the method of the present invention utilizes, in addition to group 1, group 2, and group T; a group T in which no bilinear map exists so as to use an ElGamal encrypted text in this group in place of the encrypted text used in the above described reference. The security of such ElGamal encrypted text relies on the difficulty in solving the Diffie-Hellman discrimination problem. The method of solving this problem has been studied for many years and therefore it is reasonable to consider that the problem is sufficiently difficult to solve.

In order to solve the second problem, the method of the present invention utilizes not just ElGamal encrypted text, but an ElGamal-type encrypted text which is secure against selective attacks on an encryption text.

[0036]

For the third problem, it is found that adopting the methods for solving the above described two problems would make the group signing method of the present invention more effective than related techniques.

[0037]

According to the present invention, the grounds for security do not rely on the assumption that it is difficult to solve the linear Diffie-Hellman

discrimination problem. Moreover, they do not rely on the generic group model. For these reasons, it is possible to create and verify a more secure group signature.

[0038]

The amount of calculation and the signature length required by the group signing device and the group-signature verifying device used in the present invention are compared with those of the related arts as follows.

[0039]

In the present invention, the numbers of times of scalar multiplication on group E or group 1, group 2; power modulo operation; and the calculation of bilinear map on group T, which are required by the group signing device, are respectively 7, 4 and 1, and those required by the verifying device are 6, 5 and 2. Further, the signature length is 10 times the length of p.

[0040]

In the method of related art, the scalar multiplication of group E or group 1, group 2; power modulo operation and calculation of bilinear map on group T, which are required by the group signing device, are respectively 13, 4 and 1, and those required by the verifying device are 12, 5 and 2. Also, the signature length is 12 times the length of p.

[0041]

So far as specifically described, the present invention is more effective than the method of related art.

Brief Description of the Drawings

[0042]

Figure 1 shows the configuration of the member-certificate acquiring device according to embodiment 1 of the present invention;

Figure 2 shows the configuration of the member-certificate issuing device in embodiment 2 of the present invention;

Figure 3 shows the configuration of the group signing device in embodiment 3 of the present invention;

Figure 4 shows the configuration of the group signing device in embodiment 4 of the present invention;

Figure 5 shows the configuration of the group-signature verifying device in embodiment 5 of the present invention;

Figure 6 shows the configuration of the group-signature verifying device in embodiment 6 of the present invention;

Figure 7 shows the configuration of the tracking device in embodiment 7 of the present invention; and

Figure 8 shows the configuration of the group signing system in embodiment 8 of the present invention.

Description of Symbols

[0043]

100 Member-certificate acquiring device

101 Group public key

102 Random number

103 Member-evidence generating device

104 Member evidence

107 Member secret key

108 Commitment generating device

109 Commitment

111 Challenge acquiring device

112 Challenge value

113 Response generating device

114 Response

116 Member certificate source

117 Member-certificate-source verifying device

119 Member certificate

200 Member-certificate issuing device

209 Group secret key

210 Member secret key

202 Member-evidence acquiring device

205 Challenge generating device

207 Response verifying device

208 Member-certificate-source generating device

300 Group signing device

301 Tracking public key

302 Message

303 Random number

313 Group signature

303 Encryption device using group E

304 Member-evidence encrypted text

306 Commitment generating device

307 Commitment

308 Challenge-value generating device

309 Challenge value

310 Response generating device

311 Response

312 Group-signature output device

500 Group-signature verifying device

502 Commitment generating device

503 Commitment

504 Challenge-value generating device

505 Challenge value

506 Response device

700 Tracking device

701 Tracking secret key

702 Random number

703 Decryption device using group E

704 Part of member evidence

704' Member evidence

706 Commitment generating device

707 Commitment

708 Challenge-value generating device

709 Challenge value

710 Response generating device

711 Response

712 Output device

713 Decryption validity proof

Best Mode for Carrying Out the Invention

[0044]

An exemplary embodiment of the present invention will be described in detail with reference to the appended drawings.

[0045]

First, the assumed conditions will be described.

p is a prime number.

Group 1, group 2, group T, and group E are each a group of order p.

It is assumed taht there is a bilinear map e from group 1 and group 2 to group T.

Group E is a group on which it is difficult to solve the Diffie-Hellman discrimination problem by a multiplicative group on a prime field or a general elliptic curve.

ϕ is an isomorphic map from group 2 to group 1.

Hash is a hash function which maps a letter string to field (Z/pZ).

G_2 is a generator of group 2, and G_1 is a generator of group 1 where $\phi(G_2 = G_1$.

G is a generator of group E.

H and K are randomly selected unknowns of group 1.

γ is a randomly selected unknown of field Z/pZ.

$Y = [\gamma]G_2$

s and t are randomly selected two points on field Z/pZ.

S and T are S = [s]G, T = [t]G.

The group secret key is γ.

The group public key is a letter string, which describes p, group 1, group 2, group T, bilinear map e, isomorphic map ϕ, and hash function Hash, and G_1,G_2,G,H,K,Y.

The tracking secret key is (s,t).

The tracking public key is (S,T).

[0046]

[Embodiment 1]

[Member-certificate acquiring device 100]

Figure 1 is a block diagram to show the configuration of member-certificate acquiring device 100 according to the present invention.

[0047]

Member-certificate acquiring device 100, which transmits/receives to/from member-certificate issuing device 200 to input group public key 101 and random number 102 and to output member secret key 107 and member certificate 119, comprises member-evidence generating device 103, commitment generating device 108, challenge acquiring device 111, response generating device 113, and member-certificate-source verifying device 117. Member-certificate acquiring device 100 sends member evidence 104, commitment 109, and response 114 to member-certificate issuing device 200 during the course of communication with member-certificate issuing device 200, and receives challenge value 112 and member certificate source 116.

[0048]

Moreover, member-certificate acquiring device 100 is made up of a general-purpose computer system which includes an input device, an output device, a storage device, and a control device, wherein member evidence 104, member secret key 107, commitment 109, challenge value 112, response 114, and member certificate source 116 are stored in memory. Moreover, devices other than these are virtually configured in the computer system. Further, procedure 106 described below is performed by using commitment generating device 108, commitment 109, challenge acquiring device 111, challenge value 112, response generating device 113, and response 114 out of the above described constituents.

[0049]

Member-certificate acquiring device 100 is input with group public key 101 and random number 102. Member-evidence generating device 103 randomly selects member secret key 107 (x_U) on field (Z/pZ) from input random number 102; and then from x_U, generates

$Q_U = [x_U]G$

$H_U = [x_U]H+[z'_U]K$.

This is called member evidence 104, and (Q_U,H_U) is sent to member-certificate issuing device 200.

[0050]

According to the procedure 106 described below, knowledge of (x_U,z'_U) which satisfies following two equations,

$Q_U = [x_U]G$

$H_U = [x_U]H+[z'_U]K$

is proved for the member-certificate issuing device.

[0051]

[Start of procedure 106]

Commitment generating device 108 randomly selects x'_U,z' from field (Z/pZ) from random number 102 which has been input, and generates commitment 109 that has the content described below to send to member-certificate issuing device 200.

$Q'_U = [x'_U]G$

$H'_U = [x'_U]H+[z']K$

Thereafter, member-certificate acquiring device 100 waits for challenge value 112 (c_U), which is an unknown of field Z/pZ, to be sent from member-certificate issuing device 200.

[0052]

Upon receipt of challenge value 112 (c_U), response generating device 113 calculates response 114 shown below and sends it to member-certificate issuing device 200.

$r_U = c_U x_U+x'_U$

$s_U = c_U z'_U+z'$

[End of procedure 106]

Thereafter, member-certificate acquiring device 100 waits for member certificate source 116 having a content shown below to be sent from member-certificate issuing device 200.

$y_U \in Z/pZ$,

$z''_U \in Z/pZ$,

$A_U \in$ group 1

Upon receipt of the above values, member-certificate-source verifying device 117 calculates

$z_U = z'_U + z''_U$

and after verifying that the following equation

$e(A_U, Y+[y_U]G_2) \cdot e([x_U]H, G_2) \cdot e([z_U]K, G_2) = e(G_1, G_2)$

is satisfied, uses (A_U, y_U, z_U) as member certificate 119 and outputs x_U as member secret key 107.

[0053]

[Embodiment 2]

[Member-certificate issuing device 200]

Figure 2 is a block diagram to show the configuration of member-certificate issuing device 200 according to the present invention.

[0054]

Member-certificate issuing device 200, which transmits/receives to/from member-certificate acquiring device 100 to input group public key 101, random number 102 and group secret key 209 and to output member evidence 104, comprises challenge generating device 205, response verifying device 207, member-certificate-source generating device 208, and member-evidence acquiring device 202. Member-certificate issuing device 200 sends challenge value 112 and member certificate source 116 to member-certificate acquiring

device 100 and receives member evidence 104, commitment 109 and response 114 during the course of communication with member-certificate acquiring device 100.

[0055]

Further, member-certificate issuing device 200 is made up of a general-purpose computer system which includes an input device, an output device, a storage device and a control device, wherein member evidence 104, commitment 109, challenge value 112, response 114, member certificate source 116 are stored in memory. Moreover, devices other than these are virtually configured in the computer system. Moreover, procedure 203 described below is performed by using commitment 109, challenge value 112, response 114, member certificate source 116, challenge generating device 205, response verifying device 207, and member-certificate-source generating device 208 from among the above described constituents.

[0056]

Member-certificate issuing device 200 is input with group public key 101, group secret key 209, and random number 201 and, upon start of operation, waits for member evidence 104 $(Q_U,H_U) \in$(group E, group 1) to be sent from member-certificate acquiring device 100.

[0057]

When member evidence 104 is sent from member-certificate acquiring device 100, it is verified through procedure 203 that member-certificate acquiring device 202 retains knowledge of x_U,z'_U which satisfies the following two equations.

$Q_U = [x_U]G$

$H_U = [x_U]H+[z'_U]K$

[Start of procedure 203]

Challenge generating device 205 waits for commitment 109 $((Q'_U,H'_U)\in$(group E, group 1)) to be sent from member-certificate acquiring device 100.

[0058]

When commitment 109 is sent, from input random number 201, challenge generating device 205 randomly selects challenge value 112 (c_U) from field (Z/pZ) to send to member-certificate acquiring device 100.

[0059]

Thereafter, when response 114 $((r_U,s_U) \in (Z/pZ)^{2)}$ is sent from member-certificate acquiring device 100, response verifying device 207 verifies that

$[r_U]G = [c_U]Q_U+Q'_U$

$[r_U]H+[s_U]K = [c_U]H_U+H'_U$

are satisfied.

[0060]

[End of procedure 203]

Member-certificate-source generating device 208 selects $(y_U,z''_U) \in (Z/pZ,Z/pZ)$ from the input random number to generate $A_U = [1/(\gamma+y_U)](G_1-H_U-[z''_U]K$ and sends (A_U,y_U,z''_U) to member-certificate acquiring device 100 as member certificate source 116.

Member evidence 104 (Q_U) is output.

[0061]

[Embodiment 3]

[Group signing device 300]

Figure 3 is a block diagram to show the configuration of group signing device 300 according to the present invention.

[0062]

Group signing device 300, which is input with group public key 101, group secret key 107, member certificate 116, tracking public key 301, message 302, and random number 303, and outputs group signature 313, comprises encryption device 303 using group E, member-evidence encrypted text 304, commitment generating device 306, commitment 307, challenge-value generating device 308, challenge value 309, response generating device 310, response 311, group signature output device 312.

[0063]

Moreover, group signing device 300 is made up of a general-purpose computer system which includes an input device, an output device, a storage device and a control device, wherein member-evidence encrypted text 304, commitment 307, challenge value 309, and response 311 are stored in memory. Moreover, devices other than these are virtually configured in the computer system. Further, knowledge-proof-statement generating device 305 is made up of commitment generating device 306, commitment 307, challenge-value generating device 308, challenge value 309, response generating device 310, and response 311 from among the above described constituents.

[0064]

Group signing device 300 is input with group public key 101, tracking public key 301, member certificate 116, member secret key 107, message 302 (m), and random number 303.

[0065]

Encryption device 303 using group E randomly selects q,r from field Z/pZ and generates encrypted text 304 having following content.

$B = A_U + [q]K$

$U = [x_U + r]G$

$V = [r]S$

$W = [r]T$

Successively, the following processing is performed in knowledge-proof-statement generating device 305. This processing provides proof of knowledge of $(A_U, y_U, z_U, x_U, q, r)$.

[0066]

[Start of knowledge-proof-statement generation]

By using commitment generating device 306, t,u,v,w,o are randomly selected from field Z/pZ and

$X' = e(H,G_2)^t \cdot e(B,G_2)^u \cdot e(K,G_2)^v \cdot e(K,Y)^w$

$U' = [t+o]G$

$V' = [o]S$

$W' = [o]T$

are generated to use (X',U',V',W') as commitment 307.

[0067]

Next, by using challenge-value generating device 308, challenge value 309 having the following content is generated.

$c = \mathrm{Hash}(p,G_1,G_2,G_T,G,\phi,Y,S,T,H,K,B,U,V,W,X',V',W',U',m)$

Then, using response generating device 310,

$x' = cx_U+t$

$y' = cy_U+u$

$z' = c(z_U-qy_U)+v$

$q' = -cq+w$

$r' = cr+o$

are generated to use (x,y',z',q',r') as response 311.

[0068]

[End of knowledge-proof-statement generation]

Group signing device 300 outputs (B,U,V,W,c,x',y',z',q',r') as group signature 313 for message m through group-signature output device 312.

[0069]

[Embodiment 4]

[Group signing device 400]

Figure 4 is a block diagram to show the configuration of group signing device 300 according to the present invention.

[0070]

Group signing device 400 has the same configuration as group signing device 300 shown in Figure 3 but differs only in that the group signature to be output contains commitment (B,U,V,W,X',U',V',W',x',y',z',q',r').

[0071]

[Embodiment 5]

[Group-signature verifying device 500]

Figure 5 is a block diagram to show the configuration of group-signature verifying device 500 according to the present invention.

[0072]

Group-signature verifying device 500, which is input with group public key 101, tracking public key 301, message 302, and group signature 313 and outputs valid/invalid 507, comprises commitment generating device 502, commitment 503, challenge-value generating device 504, challenge value 505, and response device 506.

[0073]

Moreover, group-signature verifying device 500 is made up of a general-purpose computer system which includes an input device, an output device, a storage device, and a control device, wherein commitment 503 and challenge

value 505 are stored in memory. Further, devices other than these are also virtually made up of in the computer system.

[0074]

Group-signature verifying device 500 is input with group public key 101, tracking public key 301, message 302 (m), and group signature 313 (B,U,V,W,c,x',y',z',q',r').

[0075]

Commitment generating device 502 generates commitment 503 (X',U',V',W') having following content.

$X' = e(H,G_2)^(x')e(B,G_2)^(y')e(K,G_2)^(z')e(K,Y)^(q')(e(G_1,G_2)/e(B,Y))^(c)$

$U' = [x'+r']G-[c]U$

$V' = [r']S-[c]V$

$W' = [r']T-[c]W$

Challenge-value generating device 504 calculates challenge value 505 having following content.

$c' = Hash(p,G_1,G_2,G_T,G,\phi,Y,S,T,H,K,B,U,V,W,X',V',W',U',m)$

Response device 506 verifies if challenge value c' generated by challenge-value generating device 504 corresponds to c included in group signature and, if there is a correspondence, outputs "valid" as the output of valid/invalid 507 and if not, outputs "invalid."

[0076]

[Embodiment 6]

[Group-signature verifying device 600]

Figure 6 is a block diagram to show the configuration of group-signature verifying device 600 according to the present invention.

[0077]

Group-signature verifying device 600, which is input with group public key 101, tracking public key 301, message 302, and group signature 313 and outputs valid/invalid 605, comprises commitment 601, challenge-value generating device 602, challenge value 603, and response device 604. Commitment 601, challenge-value generating device 602, challenge value 603, and response device 604 are similar to commitment 503, challenge-value generating device 504, challenge value 505, and response device 506 shown in Figure 5.

[0078]

The way in which group-signature verifying device 600 differs from group-signature verifying device 500 shown in Figure 5 is: that the group signature to be input is (B,U,V,W,X',U',V',W',x',y',z',q',r'); that, (X',U',V',W') included in the group signature is used as commitment 601 without using the commitment generating device; and that challenge value 603(c') which is generated by response device 604 using challenge-value generating device 602 is used and, if all of the following

$X' = e(H,G_2)^{(x')}e(B,G_2)^{(y')}e(K,G_2)^{(z')}e(K,Y)^{(q')}(e(G_1,G_2)/e(B,Y))^{(c')}$

$U' = [x'+r']G-[c']U$

$V' = [r']S-[c']V$

$W' = [r']T-[c']W$

are satisfied, "valid" is output as the output of valid/invalid 605 and, if any one of them is not satisfied, "invalid" is output.

[0079]

[Embodiment 7]

[Tracking device 700]

Figure 7 is a block diagram to show the configuration of tracking device 700 according to the present invention.

[0080]

Tracking device 700, which is input with group public key 101, tracking public key 301, message 302, group signature 313, tracking secret key 701, and random number 702 and outputs member evidence 704' and decryption validity proof 713, comprises decryption device 703 using group E, part of member evidence 704, commitment generating device 706, commitment 707, challenge-value generating device 708, challenge value 709, response generating device 710, response 711, and output device 712.

[0081]

Moreover, tracking device 700 is made up of a general-purpose computer system which includes an input device, an output device, a storage device, and a control device, wherein part of member evidence 704, commitment 707, challenge value 709, and response 711 are stored in memory. Further, devices other than these are also virtually configured in the computer system.

[0082]

Furthermore, decryption proof device 705 is made up of commitment generating device 706, commitment 707, challenge-value generating device 708, challenge value 709, response generating device 710, response 711, from among the above described constituents.

[0083]

Tracking device 700 is input with group public key 101, tracking public key 301, tracking secret key 701, message 302 (m), group signature 313 (B,U,V,W,c,x',y',z',q',r'), and random number 702.

[0084]

Decryption device 703 using group E generates part of member evidence 704 having following content,

Q = U-[1/s]V

from the encrypted text of part of member evidence and tracking secret key 701.

Commitment generating device 706 selects unknown r of field Z/pZ using random number 707 to generate commitment 707 having following content.

V" = [r]V

G" = [r]G

Challenge-value generating device 708 generates challenge value 709 having following content.

c" = Hash(p,G_1,G_2,G_T,G,ϕ,Y,S,T,H,K,B,U,V,W,X',V',W',U',m,V",G")

Response generating device 710 generates response 711 having following content.

r" = c"/s+r

Output device 712 outputs part of member evidence 704 (Q) as member evidence 704' using (V",G",r") as decryption validity proof 713.

[0085]

[Embodiment 8]

[Group signing system 800]

Figure 8 is a block diagram to show the configuration of group signing system 800 according to the present invention.

[0086]

This embodiment is a system comprising member-certificate acquiring device 100 shown in Figure 1, member-certificate issuing device 200 shown in Figure 2, group signing device 300 shown in Figure 3, group-signature verifying device 500 shown in Figure 5, and tracking device 700 shown in Figure 7. Group signing device 300 may be group signing device 400 shown in Figure 4, and also group-signature verifying device 500 may be group-signature verifying device 600.

[0087]

Member-certificate acquiring device 100 communicates with member-certificate issuing device 200 to acquire member certificate 116 and member secret key 107.

[0088]

Group signing device 300 is input with message 302, group public key 101, tracking public key 301, member certificate 116 acquired by member-certificate acquiring device 100, and acquired member secret key 107, and group signing device 300 outputs group signature 313 for message 302.

[0089]

Group-signature verifying device 500 is input with message 302, group public key 101, tracking public key 301, message 302, and group signature 313, and verifies whether group signature 313 is a valid group signature for the message, and outputs valid/invalid 605 indicating the result thereof.

[0090]

Tracking device 700 is input with tracking public key 301, group signature 313, and tracking secret key 701, and outputs member evidence 704 indicating a member who has generated the group signature.

CLAIMS

1. A member-certificate acquiring device, which is input with a group public key and a random number and outputs a member certificate and a member secret key by communicating with a member-certificate issuing device, characterized in that

when input with said group public key which includes: a description for four groups: group 1, group 2, group T, and group E, of the same order number; a description of bilinear mapping from group 1 and group 2 to group T; each generator of group 1, group 2, group T, and group E; and a signature public key of a signature scheme using said group 1, said group 2, and said group T, *said member-certificate acquiring device sends*: said member secret key including an integer not larger than said order number; a member evidence which is a value given by multiplying said generator of said group E by said member secret key; and an element of said group 1 or group 2 which is a value given by multiplying said generator of said group 1 or group 2 by said member secret key, *to* said member-certificate issuing device, and thereafter upon receipt of a signature for said member secret key, which is verifiable by said signature public key, from said member-certificate issuing device, uses said signature as said member certificate.

2. A member-certificate issuing device, which is input with a group public key, a group secret key and a random number and which outputs a member evidence for use in identifying a member by communicating with a member-certificate acquiring device, characterized in that

the member-certificate issuing device is input with said group public key which includes: a description for four groups: group 1, group 2, group T, and

group E, of the same order number; a description of bilinear mapping from group 1 and group 2 to group T; each generator of group 1, group 2, group T, and group E; and a signature public key of a signature scheme using said group 1, said group 2, and said group T, and said group secret key which includes a signature secret key corresponding to said signature public key of a signature scheme using said group 1, said group 2, and said group T, and upon receipt of member evidence which is a value given by multiplying said generator of said group E by the member secret key, and an element of said group 1 or said group 2 which is a value given by multiplying the generator of said group 1 or group 2 by the member secret key from said member-certificate acquiring device, generates a signature for said member secret key using said signature secret key to send said signature to the member-certificate acquiring device as said member certificate.

3. A group signing device, which is input with a group public key, a tracking public key, a member certificate, a member secret key, and a message and which outputs a group signature for said message, characterized in that

said group signing device comprises an encryption device for creating an encrypted text in which part of the member evidence generated from the member secret key is encrypted by the tracking public key from: said group public key including a description for four groups: group 1, group 2, group T, and group E, of the same order number, a description of bilinear mapping from group 1 and group 2 to group T, each generator of group 1, group 2, group T, and group E, a signature public key of a signature scheme utilizing said group 1, said group 2, and said group T; said tracking public key comprising an element of said group E; and said member secret key.

4. The group signing device according to claim 3, characterized in that said group signing device comprises a knowledge-proof-statement generating device which generates a knowledge proof statement which is data for proving that a secret key encrypted into said encrypted text and a signature for said secret key can be calculated from input data, wherein said group signature to be output includes a knowledge proof statement generated by said knowledge-proof-statement generating device.

5. The group signing device according to claim 4, characterized in that said knowledge-proof-statement generating device comprises:

a commitment generating device which is input with said group public key, said tracking public key, said member secret key, said member certificate, and said random number and generates a commitment to encryption which is data for proving knowledge of a random number for encryption, and a commitment to a member certificate which is data for proving knowledge of a signature and member secret key, to output said commitment to encryption and said commitment to a member certificate as a commitment;

a challenge-value generating device which is input with said group public key, said tracking public key, said encrypted text, and said commitment and outputs a hash value of the foregoing values as a challenge value; and

a response generating device which is input with said group public key, said member secret key, said member certificate, said random number, and said challenge value, and outputs a response of encryption and a response of member certification as a response.

6. The group signing device according to claim 5, characterized in that

said group signature comprises said encrypted text, said commitment, and said response.

7. The group signing device according to claim 5, characterized in that

said group signature comprises said encrypted text, said challenge value, and said response.

8. A group-signature verifying device, which is input with a group public key, a tracking public key, a message, and a group signature, and judges whether said group signature is a valid group signature for said message to output "valid" or "invalid," wherein

when input with: a group public key which includes a description for four groups: group 1, group 2, group T, and group E, of the same order number; a description of bilinear mapping from group 1 and group 2 to group T; each generator of group 1, group 2, group T, and group E; and a signature public key of a signature scheme using said group 1, said group 2, and said group T; a tracking public key comprising an element of group E; and a group signature including an encrypted text in which part of member evidence generated by a member secret key is encrypted by the tracking public key, said group-signature verifying device judges whether said group signature is a valid group signature for said message to output "valid" or "invalid."

9. The group-signature verifying device according to claim 8, characterized in that

said group-signature verifying device comprises a knowledge-proof-statement verifying device which verifies that a knowledge proof statement is data to prove that a secret key which is used to generate part of member

evidence encrypted into said encrypted text, and a signature for the secret key can be calculated from data input into the group signing device and from data included in the group signing device, and

said group signature includes a knowledge proof statement which has been verified by said proof-statement verifying device.

10. The group signing device according to claim 9, characterized in that

said group signature comprises said encrypted text, said commitment, and said response, and

said knowledge-proof-statement verifying device comprises:

a challenge-value generating device which is input with said group public key, said tracking public key, said encrypted text, and said commitment, and outputs a hash value of the foregoing values as a challenge value; and

a response verifying device which is input with said group public key, said tracking public key, said encrypted text, said commitment, said challenge value and said response, and outputs "valid" or "invalid" depending on whether or not these inputs satisfy a given equation, wherein

the output of said response verifying device is output as the output of said group-signature verifying device.

11. The group-signature verifying device according to claim 9, characterized in that:

said group signature comprises said encrypted text, said challenge value, and said response; and

said knowledge-proof-statement verifying device comprises:

a commitment generating device which is input with said group public key, said tracking public key, said response, and said challenge value, and

outputs a commitment to encryption and a commitment to member certificate as a commitment; and

a response verifying device which is input with said public key, said tracking public key, said encrypted text, and said commitment, and outputs "valid" or "invalid" depending on whether or not a hash value of the foregoing values corresponds to said challenge value, wherein

the output of said response verifying device is output as the output of the group-signature verifying device.

12. A tracking device, which is input with a group public key, a tracking public key, a group signature, and a tracking secret key, and which decrypts the encrypted text of part of the member evidence generated from a member secret key contained in the group signature to output the part of member evidence which is a value uniquely determined from the member secret key.

13. A group signing system, comprising the member-certificate acquiring device according to claim 1, the member-certificate issuing device according to claim 2, the group signing device according to claim 3, the group-signature verifying device according to claim 8, and the tracking device according to claim 13, characterized in that

said member-certificate acquiring device communicates with said member-certificate issuing device to acquire a member certificate and a member secret key; inputs the acquired said member certificate, the acquired said member secret key, a message, a group public key, and a tracking public key into said group signing device to acquire a group signature for said message; and inputs said message and the acquired group signature into said group-signature verifying device to verify that the acquired group signature is a

valid group signature for said message and to input said group signature into said tracking device thereby outputting a member evidence representing the member which has generated the group signature.