A NEW SCHEME FOR ID-BASED CRYPTOSYSTEM AND SIGNATURE

CHI SUNG LAIH*, JAU YIEN LEE*, LEIN HARN**, and CHIN HSING CHEN*

* Department of Electrical Engineering,
National Cheng Kung University
Tainan, Taiwan, R.O.C.

** Computer Science Program,
University of Missouri,
Kansas City, Mo 64110, U.S.A

ABSTRACT

This paper proposes a new ID-based cryptographic scheme for implementing public-key cryptosystem and signature. Instead of generating and publishing a public key for each user, the ID-based scheme permits each user to choose his name or network address as his public key. This eliminates the needs of a large public-file and the exchange of private or public keys. The major advantage of the ID-based cryptosystem based on our scheme over other published ID-based cryptosystems is that the number of users can be extended to t*L users without degrading the system's security even when users cospire, where L is the number of the system's secrets and t is the number of factors in p-1.

I. Introduction

The concept of identity-based (ID-based) cryptosystem and signature scheme were first proposed by Shamir in 1984 [1]. The ID-based cryptosystem is similar to the well-known public key cryptosystem. However, ID-based cryptosystems have the attractive feature that instead of using a large random number as each user's public-key, each user can choose his name, telephone number, social security number, office address etc., as his public key. Therefore, ID-based cryptosystems enable any pair of users to communicate securely without keeping a large public file directory, without exchanging private or public keys, and without using services provided from a third party.

In an ID-based cryptosystem, we assume the existence of a trusted key generation center. The center provides each user a smart card when he first joins the network. The information embedded in his card enable the user to sign and encrypt the message he wishes to send and to decrypt and verify the messages he received. When a new user joins the network, previously issued cards need not to be updated. After all the users have joined the network, the center can be closed and the network continues to work for an indefinite period.

Like the concept of public-key cryptosystem proposed by Diffie and Hellman [2], Shamir did not present how to implement an ID-based cryptosystem. Instead, he proposed an ID-based signature scheme and conjectured the existence of ID-based cryptosystems. In 1987, Tsujii et al. [3] proposed an ID-based cryptosystem which is one of the earliest realizations of Shamir's idea. However, in their system, a conspiracy of L (›n, where n is the bit number of GF(p)) users may derive the center's secret information. This renders the cryptosystem no security at all!! Therefore, in order to preserve the system's security, the number of users is constrained to be smaller than n. Under this constraint, the number of public information in the network is larger than the number of users and the system becomes not an ideal ID-based cryptosystem. To remedy this drawback, Laih and Lee [4] proposed a modified version of the Tsujii's ID-based cryptosystem lately. However, it is recently shown that the modified version is not secure when n+1 users conspire [7].

In this paper, we proposed a new ID-based cryptographic scheme. This scheme does not need a large public file nor exchange of private/public keys. The number of users can be increased to t*L without the threatening of forming conspiracy, where L is the number of system's secrets and t is the number of factors of p-1. We will show that the public-key cryptosystem and signature scheme proposed by El-Gamal can be implemented by using our proposed scheme.

This work was sponsored by Taiwan International Standard Electronics Ltd.

CH2702-9/89/0000/0998$01.00 © 1989 IEEE

First, we will review both the Diffie-Hellman public key distribution system [2] and the El-Gamal public key cryptosystem and signature scheme [5]. In section III, we introduce a new ID-based cryptographic scheme. In section IV, we implement the El-Gamal's public key cryptosystem by using our proposed scheme. The implementation of the El-Gamal's signature system with our proposed scheme is presented in section V. Conclusion and remarks are found in section VI.

II. Review of public-key system

A. The Diffie-Hellman public key distribution system [2]:

Suppose user A and user B want to share a secret K_{AB}, where A has a secret x_A and B has a secret x_B. Let p be a large prime number and α be a primitive element over GF(p), both are known to all users. A computes $y_A = \alpha^{x_A}$ mod p and sends y_A to B or stores y_A in a public file. Similarly, B computes a public key $y_B = \alpha^{x_B}$ mod p, and sends y_B to A or stores y_B in the public file. Then the common secret K_{AB} shared by A and B is given by

$$\begin{aligned} K_{AB} &= y_A^{x_B} \mod p \\ &= y_B^{x_A} \mod p \\ &= \alpha^{x_A x_B} \mod p \qquad (1) \end{aligned}$$

For an intruder, he only knows y_A, y_B, α and p. If he wants to compute K_{AB}, it is believed to be equivalent to computing discrete logarithms over finite fields.

For any cryptographic system based on the difficulty of computing discrete logarithm, p must be chosen such that p-1 has at least one large prime factor. If p-1 has only small prime factors, then computing discrete logarithm becomes easy [6]. Throughout this paper, we assume $p-1 = 2p_1p_2 \cdots p_t$, where p_is are another large prime numbers.

B. The El-gamal's public-key cryptosystem [5]:

Suppose user A wants to send user B a message m, where $0 \le m \le p-1$. A chooses a random number r ($0 \le r \le p-2$) and computes the ciphertext C as follows:

$$C = (c_1, c_2), \qquad (2)$$

$$c_1 = \alpha^r \mod p, \qquad (3)$$

$$c_2 = m(y_B)^r \mod p. \qquad (4)$$

When B receives the ciphertext C, he computes

$$(c_1)^{x_B} = (\alpha^r)^{x_B} = (\alpha^{x_B})^r = y_B^r \mod p. \quad (5)$$

B recovers the message m by computing

$$\begin{aligned} (c_1^{x_B})^{-1} c_2 &= (y_B^r)^{-1} m (y_B)^r \mod p \\ &= m \mod p. \qquad (6) \end{aligned}$$

It is not advisable to use the same value r for enciphering more than one block of the message. Also note that breaking El-Gamal's public key cryptosystem is equivalent to breaking the Diffie-Hellman key distribution system. For more details refer to [5].

C. The El-Gamal's public-key signature scheme [5]:

Let m be a document that user A wants to sign, where $0 \le m \le p-1$. A first chooses a random number k ($0 \le k \le p-1$) such that GCD (k, p-1)=1. A computes

$$r = \alpha^k \mod p. \qquad (7)$$

Then A computes another number s by solving

$$m = x_A r + ks \mod p-1. \qquad (8)$$

Since GCD(k, p-1)=1, s can be uniquely determined in Eq.(8). The signature for m is the pair (r, s), $0 \le r$, $s \le p-1$. Given m, r and s, each user can easily verify the authenticity of the signature by checking if

$$\begin{aligned} \alpha^m &= y_A^r * r^s \mod p \\ &= \alpha^{x_A r + ks} \mod p. \qquad (9) \end{aligned}$$

is satisfied.

Note that although it has not yet been proven that breaking the El-Gamal's signature scheme is equivalent to solving discrete logarithms. Some attacks to this scheme were discussed in [5]. None of them seems to break the system.

III. A new ID-based cryptographic scheme

The ID-based system assumes the existence of a trusted key generation center whose purpose is to provide secrets to each user when he first joins the network. Each user has a q-bits number as his ID number (e.g., q=100). The ID number can be a combination of name, social security number, office number or telephone number. When each user registers his ID number with the trusted center, the center stores it in a public file. The center then publishes a one-to-one, one way function f(.) (e.g., RSA). Any user can compute user S's extended ID, EID_S, by the following:

$$ID_S=(x'_{S1}, x'_{S2}, \ldots, x'_{Sq}), \tag{10a}$$

$$\begin{aligned} EID_S &= f(ID_S) \\ &= (x_{S1}, x_{S2}, \ldots, x_{Sn-1}, x_{Sn}), \ q<n, \end{aligned} \tag{10b}$$

where $x_{Si} \in \{0, 1\}$, $1 \le i \le n-1$, and $x_{Sn}=0$ for $\sum_{i=1}^{n-1} x_{Si}$ is odd number, $x_{Sn}=1$ for $\sum_{i=1}^{n-1} x_{Si}$ is even number.

The EID likes a long pseudo-random number which prevents a countermeasure against conspiracy among some users. The center chooses an arbitrary large prime number p and generates two vectors B and C satisfying

$$B=(b_1, b_2, \ldots, b_n), \ 1 \le b_i \le p-2, \ 1 \le i \le n,$$
$$b_i \text{ are odd numbers.} \tag{11a}$$

$$C = (c_1, c_2, \ldots, c_q), \ 1 \le c_i \le p-2, \ 1 \le i \le q, \tag{11b}$$

$$B \bullet EID_i \neq B \bullet EID_j \bmod p-1, \text{ if } EID_i \neq EID_j, \tag{12a}$$

$$C \bullet ID_i \neq C \bullet ID_j \bmod p-1, \text{ if } ID_i \neq ID_j, \tag{12b}$$

where EID_i, EID_j are the expanded IDs of user i and user j. As defined in Eq.(10b), since EID has odd number of 1s, if we choose b_is to be all odd numbers then B•EID mod p-1 is almost relatively prime to p-1 when the number of users is small compared to p-1.

Now, the center chooses an integer which is a primitive element mod p. The center then computes two vectors Y and Z by

$$Y = (y_1, y_2, \ldots, y_q), \tag{13a}$$

$$Z = (z_1, z_2, \ldots, z_n), \tag{13b}$$

$$y_i = \alpha^{c_i} \bmod p, \ i=1, 2, \ldots, q, \tag{14a}$$

$$z_i = \alpha^{b_i} \bmod p, \ i=1, 2, \ldots, n. \tag{14b}$$

Then the center divides all users into t groups, where t is the number of factors in p-1 which is defined in section II. Each group has L=n+q users. Each user knows that all the other users belong to. If user S registers to the system, the center issues a smart card to user S after properly verifies his physical identity. The smart card includes the set of integers (p, p_i, $1 \le i \le t$, Y, Z, K_S), where p, p_i, $1 \le i \le t$, Y, Z are common to all users while K_S is known only to user S. Numbers c_j, $1 \le j \le q$, b_i, $1 \le i \le n$, can be aborted after all cards has been issued. If there is no more new user, the center can be closed. Hence, c_j, $1 \le j \le q$, b_i, $1 \le i \le n$ are kept secret from all users. The user S's secret, K_S, can be calculated by

$$K'_S = K_S \bmod p_j = ap_j + K_S, \tag{15}$$

where a is an integer and j is the group to which user S belongs and K_S can be computed by

$$C \bullet ID_S = (B \bullet EID_S)K'_S \bmod p-1 \tag{16}$$

$$\sum_{i=1}^{q} c_i x'_{Si} = (\sum_{i=1}^{n} b_i x_{Si})K'_S \bmod p-1, \tag{17}$$

Since $(B \bullet EID_S)$ is almost relatively prime to p-1, K_S can be uniquely determined. Every user can obtain user S's public key y_S and base α_S from common public information p, p_j, Z, and Y by

$$y_S = \left(\prod_{i=1}^{q} y_i^{x'_{Si}}\right)^{\frac{p-1}{p_j}} = \left(\alpha^{C \bullet ID}\right)^{\frac{p-1}{p_j}} \bmod p, \tag{18}$$

$$\alpha_S = \left(\prod_{i=1}^{n} (z_i)^{x_{Si}}\right)^{\frac{p-1}{p_j}} = \left(\alpha^{B \bullet EID}\right)^{\frac{p-1}{p_j}} \bmod p, \tag{19}$$

where x'_{Si}, x_{Si} are defined by Eq.(10).

From Eqs. (13)-(19), we obtain

$$\begin{aligned} y_S &= \left(\prod_{i=1}^{q} y_i^{x'_{Si}}\right)^{(p-1)/p_j} \\ &= \left(\prod_{i=1}^{n} z_i^{x_{Si}\, K'_S}\right)^{(p-1)/p_j} \\ &= \left(\alpha^{(\Sigma b_i x_{Si})K'_S}\right)^{(p-1)/p_j} = \alpha_S^{K_S} \bmod p \end{aligned} \tag{20}$$

Note that although α_S is not a primitive root over GF(p), it is infeasible to compute K_S from $y_S = \alpha_S^{K_S} \bmod p$ if p_j is a large prime number [6]. In our scheme, for each user S using different base α_S, the security can be increased without increasing the memory size of public file as suggested by El-Gamal [5].

Remarks:

1. If an intruder wants to compute the center's secret c_i, $1 \le i \le q$, b_i, $1 \le i \le n$, from common public information, it is equivalent to computing discrete logarithms.

2. If an intruder wants to compute user S's secret K_S from y_S, α_S and p, it is also equivalent to solving discrete logarithms.

3. L users in the same group j may conspire to derive the center's secret b_i, $1 \le i \le n$, c_i, $1 \le i \le q$ by solving L equations of the form of Eqs.(17). They are listed as follows:

$$[x_{11}'c_1+x_{12}'c_2+\ldots+x_{1q}'c_q$$
$$=(x_{11}b_1+x_{12}b_2+\ldots+x_{1n}b_n)K_1 \bmod p-1] \bmod p_j$$
$$[x_{21}'c_1+x_{22}'c_2+\ldots+x_{2q}'c_q$$
$$=(x_{21}b_1+x_{22}b_2+\ldots+x_{2n}b_n)K_2 \bmod p-1] \bmod p_j$$
$$\vdots$$
$$[x_{L1}'c_1+x_{L2}'c_2+\ldots+x_{Lq}'c_q$$
$$=(x_{L1}b_1+x_{L2}b_2+\ldots+x_{Ln}b_n)K_L \bmod p-1] \bmod p_j \quad (21)$$

Since $p_j|(p-1)$, Eq. (21) can be reformulated as the following form :

$$x_{11}'c_1+x_{12}'c_2+\ldots+x_{1q}'c_q$$
$$=(x_{11}b_1+x_{12}b_2+\ldots+x_{1n}b_n)K_1 \bmod p_j$$
$$x_{21}'c_1+x_{22}'c_2+\ldots+x_{2q}'c_q$$
$$=(x_{21}b_1+x_{22}b_2+\ldots+x_{2n}b_n)K_2 \bmod p_j$$
$$\vdots$$
$$x_{L1}'c_1+x_{L2}'c_2+\ldots+x_{Lq}'c_q$$
$$=(x_{L1}b_1+x_{L2}b_2+\ldots+x_{Ln}b_n)K_L \bmod p_j \quad (22)$$

If $GCD(b_n \bmod p_j,\ p_j)=1$ (the probability that $GCD(b_n \bmod p_j,\ p_j) \neq 1$ is very small), then there exists b_n^{-1} (mod p_j). Multiplying both sides of Eq.(22) by b_n^{-1}, we have

$$x_{11}'c_1'+x_{12}'c_2'+\ldots+x_{1q}'c_q'$$
$$=(x_{11}b_1'+x_{12}b_2'+\ldots+x_{1n}\ 1)K_1 \bmod p_j,$$
$$x_{21}'c_1'+x_{22}'c_2'+\ldots+x_{2q}'c_q'$$
$$=(x_{21}b_1'+x_{22}b_2'+\ldots+x_{2n}\ 1)K_2 \bmod p_j,$$
$$\vdots$$
$$x_{L1}'c_1'+x_{L2}'c_2'+\ldots+x_{Lq}'c_q'$$
$$=(x_{L1}b_1'+x_{L2}b_2'+\ldots+x_{Ln}\ 1)K_L \bmod p_j. \quad (23)$$

where $c_i'=c_ib_n^{-1}$ (mod p_j), $1 \le i \le q$, and $b_g'=b_gb_n^{-1}$ (mod p_j), $1 \le g \le n-1$. The reformulation of Eq.(23) yields

$$\begin{bmatrix} x_{11}' & x_{12}' & \cdots & x_{1q}' & -x_{11}K_1 & -x_{12}K_1 & \cdots & -x_{1,n-1}K_1 \\ x_{21}' & x_{22}' & \cdots & x_{2q}' & -x_{21}K_2 & -x_{22}K_2 & \cdots & -x_{2,n-1}K_2 \\ & & \vdots & & & & & \vdots \\ x_{L1}' & x_{L2}' & \cdots & x_{Lq}' & -x_{L1}K_L & -x_{L2}K_L & \cdots & -x_{L,n-1}K_L \end{bmatrix}$$
$$\begin{bmatrix} C'^T \\ \\ B'^T \end{bmatrix} = \begin{bmatrix} x_{1n}K_1 \\ x_{2n}K_2 \\ \vdots \\ x_{Ln}K_L \end{bmatrix} = [X][C',\ B'] \bmod p_j \quad (24)$$

If $GCD(|X|,\ p_j)=1$, then we can uniquely calculate C' and B'. Then all conspirators i $(1 \le i \le L)$ in the same group j can find entity h's secret-key K_h $(h > L)$ by

$$K_h = (x_{h1}'c_1'+x_{h2}'c_2'+\ldots+x_{hq}'c_q')$$
$$*(x_{h1}b_1'+x_{h2}b_2'+\ldots+x_{hn}1)^{-1} \bmod p_j \quad (25)$$

This implies that L users in the same group j can recover message from user h in the same group j. However, they cannot derive any user's secret key which is in another group since the modulo is different.

From above discussions we know that our proposed scheme has the following features :

(a) For some users have very low tendency of conspiracy, the registration center can assign these users into the same group without degrading system's security.

(b) For some users have high tendency of conspiracy, the regietration center can assign these users into different groups such that the system's security can be improved.

(c) The registration center always can create dummy users in each group to prevent user's conspiracy.

IV. An ID-based cryptosystem based on El-Gamal's public key cryptosystem

Let m ($0 \le m \le p-1$) be the message that user T wants to transmit to user S. User T first computes user S's public key y_S and base α_S from ID_S and the public information in his smart card. He then generates a random number r ($0 \le r \le p-2$) and computes the ciphertext C as follows:

$$C = (c_1, c_2). \tag{26}$$

$$c_1 = \alpha_S^{r} \mod p. \tag{27}$$

$$c_2 = m(y_S)^{r} \mod p. \tag{28}$$

User T sends the ciphertext C to user S via an insecure channel. When user S receives the ciphertext C, he computes

$$(c_1)^{K_S} = (\alpha_S^{r})^{K_S} \mod p. \tag{29}$$

Then user S recovers the message m by computing

$$\begin{aligned}(c_1^{K_S})^{-1} * c_2 & \\ &= (\alpha_S^{K_S * r})^{-1} * m * (y_S)^{r} \mod p \\ &= m \mod p. \end{aligned} \tag{30}$$

Note that this system is superior to the public-key system because it does not need a large public file.

As in the El-Gamal's public key cryptosystem, it is not advisable to use the same r for enciphering more than one block of the message. It is easy to observe that breaking this system is equivalent to computing discrete logarithms.

V. An ID-based signature scheme based on El-Gamal's public-key signature scheme

Let m ($0 \le m \le p-1$) be a document that user S wants to sign. User S first computes his public key y_S and base α_S (as given in Eqs. (16) and (17) from the public information in his smart card). S then chooses a random number k ($0 \le k \le p-2$) with GCD(k, p-1)=1 and computes

$$r = \alpha_S^{k} \mod p \tag{31}$$

and
$$m = K_S r + kz \mod p-1 \tag{32}$$

The signature for m is the pair (r, z), $0 \le r, z \le p-1$. Since each user can compute y_S and α_S, he can easily check whether

$$\begin{aligned}\alpha_S^{m} &= y_s^{r} * r^{z} \mod p \\ &= \alpha_S^{K_S r + kz} \mod p \end{aligned} \tag{33}$$

is satisfied.

VI. Conclusions and Remarks

In this paper, a new ID-based cryptographic scheme is proposed. The scheme can be used to implement cryptosystem and signature. However, it does not need a large public-file or the exchange of private/public keys. Instead, each user has a personal smart card storing the public information and his private keys. The number of users can be extened to t*L users without the threatening of forming conspiracy where L is the number of system's secret key and t is the number of factors of p-1.

The major difficulty of implementing an ID-based cryptosystem is to design a system which can prevent conspiracy from its users whose number is much large than the number of the system's secrets. Our proposed cryptosystem cannot satisfy the above general requirement. However, the users can be partitioned into different groups instead and the system's security can be improved by using our scheme. The partition strategy needs to be further studied.

Acknowledgment

The authors would like to thank Prof. T. Itoh for proposing Remark 3 described in section III.

References

[1] A. Shamir, "Identity-based cryptosystem and signature scheme," Advance in cryptology-crypto, 84, pp.47-53, 1984.

[2] W. Diffie and M.E. Hellman, "new directions in cryptography," IEEE Trans. on Inform. Theory, vol.IT-22, pp.644-654, 1976.

[3] S. Tsujii, T. Itoh and K. Kurosawa, "ID-based cryptosystem using discrete logarithm problem," Electron. Lett. vol.23, pp.1318-1320, 1987.

[4] C.S. Laih and J.Y. Lee, "A modified ID-based cryptosystem using discrete logarithm problem," Electron. Lett., vol.24, no.14, pp.858-859, 1988.

[5] T. El-Gamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. on Inform. Theory, vol.IT-31, pp.469-472, 1985.

[6] S. Pohlig and M.E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," IEEE Trans, on Inform. Theory, vol.IT-24, pp.106-110, 1978.

[7] S. Tsujii, T. Itoh, and H. Tanaka, "A note on laih and Lee's ID-based cryptosystem," to be appear on Electronics Letters.