A REALIZATION SCHEME FOR THE IDENTITY-BASED CRYPTOSYSTEM

Hatsukazu TANAKA
Department of Electrical Engineering
Kobe University
Rokko, Nada, Kobe 657, JAPAN

Abstract

At the Crypto'84, Shamir has presented a new concept of the identity-based cryptosystem, but no idea is presented on the realization scheme. In this paper a new realization scheme of the modified identity-based cryptosystem has been proposed. The basic idea of the scheme is based on the discrete logarithm problem and the difficulty of factoring a large integer composed of two large primes. The scheme seems to be very secure if all members of the system keep their secret keys safe, but if a constant number of users conspire, the center secret will be disclosed. Then it has a close relation to the well-known "threshold scheme". To cope with the conspiracy, the basic system is extended to get a new scheme of which "threshold" becomes higher. Detail considerations on the scheme are also given.

I. Introduction

At the Crypto '84, Shamir[1] has presented a new concept of the identity-based cryptosystems and signature schemes. He has proposed himself a realization scheme of the new concept of signature, but no idea is presented on a realization scheme of the identity-based cryptosystem. In this paper, modified it slightly without changing the basic important functions, a realization scheme is proposed. The basic idea of the scheme is based on the two well-known one-way functions, i.e. a factorization of a large integer composed of two large primes, and a discrete logarithm. The scheme is very simple, but it is possible to realize the Shamir's concept of the identity-based cryptosystem perfectly if all members of the system protect their secret informations safe. However, the original scheme has a crucial problem such that the center secret can be disclosed if some users conspire, because the scheme resembles to the well-known secret sharing system [2,3], i.e. a "threshold scheme". In order to overcome such a difficult problem, we extend the original scheme to a new one by introducing a new concept of "user's group" and "exchange", where the secret informations of two users are exchanged if their group numbers

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 340-349, 1988.
© Springer-Verlag Berlin Heidelberg 1988

are different. As a result the threshold number of users necessary for conspiracy will be increased, and hence, the amount of calculations to raise the threshold can be decreased.

II. Identity-Based Cryptosystem

First we introduce the Shamir's original concept of identity-based cryptosystem which enables any pair of users to communicate securely, without exchanging private or public keys, without keeping any directories, and without using the services of a third party. The scheme assumes the existence of trusted key generation center, whose sole purpose is to give each user a personalized smart card when he first joins the network. The information embedded in this card enables the user to encrypt the messages he sends and to decrypt the messages he receives in a totally independent way, regardless of the other party. Previously issued cards do not have to be updated when new users join the network, and the various centers do not have to coordinate their activities or even to keep a user list. The centers can be closed after all the cards are issued, and the network can continue to function in a completely decentralized way for an infinite period. The block diagram of this concept is shown in Fig.1.

However, it seems to be very difficult to realize the original concept directly. Then with slight modification without changing the basic important functions of the cryptosystem, a new modified cryptosystem as shown in Fig.2 is obtained, and a realization scheme is proposed in the following Chapters.

III. A Realization Scheme

A)Basic System

Let p and q be two large primes and their product be n=pq of which the Euler's totient function is given by $\Phi(n)=(p-1)(q-1)$. Let t be an arbitrary but not small positive integer, and let g be an integer which has a large period and satisfies $\max\{p,q\} < g < n$. Then select any t integers $x_\ell (1 \leq \ell \leq t)$ such that $\max\{p,q\} < x_\ell < \Phi(n)$, and assume that a user j's identity number is ID_j which is uniquely expanded to a large integer e_j using a one-way function f, i.e. $e_j=f(ID_j)$. Here the center calculates a set of the following t integers $S_{j\ell} (1 \leq \ell \leq t)$ less than n and sends it to j.

$$S_{j\ell} = g^{d_j x_\ell} \pmod{n}, \quad 1 \leq \ell \leq t \tag{1}$$

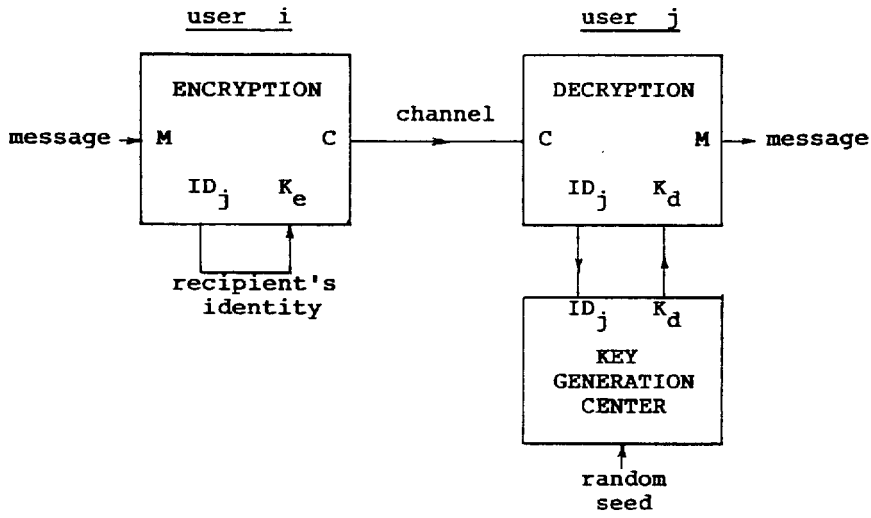

Fig.1 The Shamir's original identity-based cryptosystem.

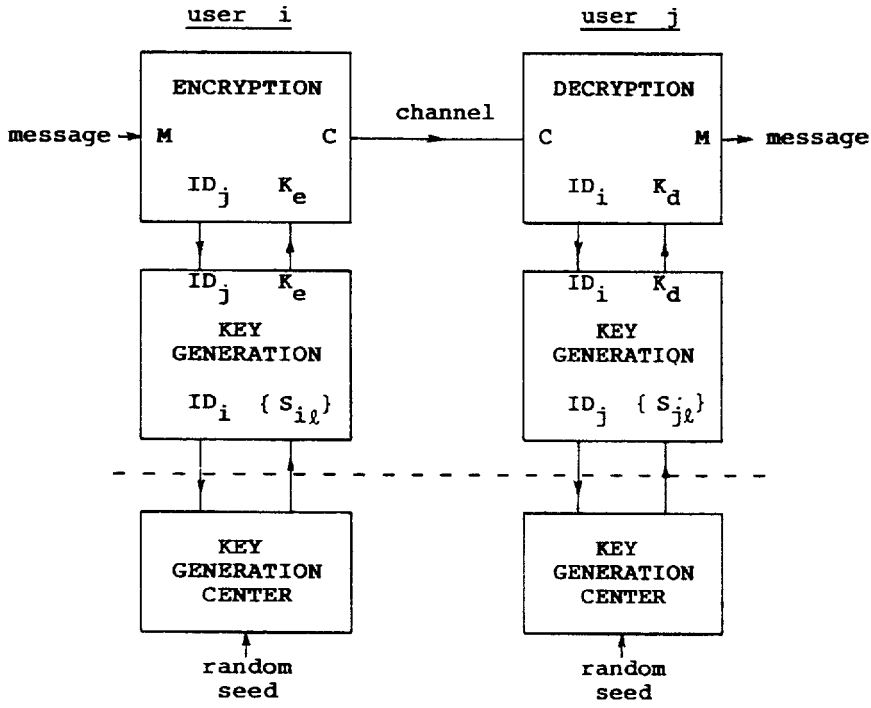

Fig.2 A modified identity-based cryptosystem.

where

$$f_{j\ell} = e_j^{\ell} \pmod n = \{f(ID_j)\}^{\ell} \pmod n \qquad (2)$$

and

$$d_j = \sum_{\ell=1}^{t} x_\ell f_{j\ell} \pmod{\Phi(n)} \qquad (3)$$

The system parameters are summarized as follows.

Center { Public-Key $K_{CP} = \{ n, t, f \}$
Secret-Key $K_{CS} = \{ p, q, g, x_\ell (1 \le \ell \le t) \}$

User j { Public-Key $K_{Pj} = \{ ID_j \}$
Secret-Key $K_{Sj} = \{ S_{j\ell} (1 \le \ell \le t) \}$

B)Common-Key Generation

When a user i wants to generate a common-key with a user j, i calculates

$$K_{ij}^{(i)} = \prod_{\ell=1}^{t} S_{i\ell}^{f_{j\ell}} \pmod n \qquad (4)$$

using his secret key $K_{Si} = \{ S_{i\ell} (1 \le \ell \le t) \}$ and j's public key $K_{Pj} = \{ID_j\}$, where

$$f_{j\ell} = \{f(ID_j)\}^{\ell} \pmod n, \quad 1 \le \ell \le t \qquad (5)$$

And when a user j wants to generate a common-key with a user i, j calculates

$$K_{ji}^{(j)} = \prod_{\ell=1}^{t} S_{j\ell}^{f_{i\ell}} \pmod n \qquad (6)$$

using his secret key $K_{Sj} = \{S_{j\ell} (1 \le \ell \le t)\}$ and i's public key $K_{Pi} = \{ ID_i \}$, where

$$f_{i\ell} = \{f(ID_i)\}^{\ell} \pmod n, \quad 1 \le \ell \le t. \qquad (7)$$

Here we must show $K_{ij}^{(i)} = K_{ji}^{(j)}$ so that two users i and j may succeed to obtain a common-key.

Theorem 1. $$k_{ij}^{(i)} = k_{ji}^{(j)} = g^{d_i d_j} \pmod n \qquad (8)$$

Proof: We will examine that the same expression can be derived by transforming $k_{ij}^{(i)}$ and $k_{ji}^{(j)}$ using Eqs.(1),(2)and (3).

$$k_{ij}^{(i)} = \prod_{\ell=1}^{t} S_{i\ell}^{f_{j\ell}} \pmod n = \prod_{\ell=1}^{t} g^{d_i x_\ell f_{j\ell}} \pmod n$$

$$= g^{d_i \sum_{\ell=1}^{t} x_\ell f_{j\ell}} \pmod n = g^{d_i d_j} \pmod n,$$

and

$$k_{ji}^{(j)} = \prod_{\ell=1}^{t} S_{j\ell}^{f_{i\ell}} \pmod n = \prod_{\ell=1}^{t} g^{d_j x_\ell f_{i\ell}} \pmod n$$

$$= g^{d_j \sum_{\ell=1}^{t} x_\ell f_{i\ell}} \pmod n = g^{d_i d_j} \pmod n.$$

Hence,

$$k_{ij}^{(i)} = k_{ji}^{(j)} = g^{d_i d_j} \pmod n. \qquad \text{(Q.E.D.)}$$

From the above theorem, we denote the common-key with

$$k_{ij} = g^{d_i d_j} \pmod n. \tag{9}$$

Remark : If a user j generates a common-key with himself using his public-key, he can obtain a key

$$k_{jj} = g^{d_j^2} \pmod n. \tag{10}$$

which has an important application to encipher his private database or to generate a conference key.

C) Enciphering and Deciphering

Once a common key between a pair of users i and j is generated, the enciphering and deciphering can be performed using the well-known algorithm of common-key cryptosystem such as DES[4] or FEAL[5].

IV. Considerations on Security

The realization scheme proposed above seems to be secure if all members of the system protect their secret keys safe. However, if a number of users conspire, the center secret will be disclosed. Then it is very important for us to consider the algorithm to extract the center secret and the number of users who should join a conspiracy for success. Concerning it the following two theorems are established, though their proofs will be given later in the full paper.

Theorem 2. If the number of users who join a conspiracy is less than t, the center secret can not be disclosed. That is, the number of users T must satisfy $T \geq t$ in order to succeed in any conspiracy.

Theorem 3. When a factorization of n=pq or its equivalent information is given, the center secret can be disclosed if T=t users conspire.

It is very interesting to notice that the above theorem clearly shows that the center secret is delivered according to the well-known "threshold scheme" with a threshold value t. Therefore it is desirable to select t as large as possible from the point of security.

Generally, a factorization of n is unknown because two primes p and q are the center secret. Under this condition the following conjecture is established on the number of users to succeed for obtaining the center secret by a user's conspiracy.

Conjecture. When a factorization of n=pq or its equivalent information is not known, the center secret can not be disclosed if the number of users who join a conspiracy is less than t+1 for $t \geq 1$, i.e. the threshold value for success in a conspiracy is t+1.

It is desirable to select t as large as possible to protect the center secret from the user's conspiracy, but the necessary amount of memory capacity to store the users secret $S_{j\ell}$ $(1 \leq \ell \leq t)$ is $t\lceil \log_2 n \rceil$ (bits), where $\lceil\ \rceil$ shows the ceiling function, and increases as t becomes larger. Hence, the maximum number of possible users to keep the network system secure for any user's conspiracy and the amount of necessary memory capacity are exchanged.

V. Extension of the Basic System

In order to increase the number of users to join a network of the identity-based cryptosystem proposed above, it is necessary to select a parameter t large enough to prohibit the user's conspiracy. However, when t increases by a factor M, the number of necessary computations to generate a common-key also increases by a factor M.

In this Chapter we extend the basic system to get a new scheme which can keep our system secure against the user's conspiracy by pulling up the "threshold". The scheme introduces a new concept of "user's group" determined uniquely by the user's identity number ID, and exchanges the user's secret information between any two users in the different groups with no interaction and without leakage of any knowledge on their secret informations.

Let M be the number of user's groups and c be any positive integer. Then the group number N $(0 \leq N \leq M-1)$ of a user j is determined by

$$N = \{e_j\}^c \pmod{M} = \{f(ID_j)\}^c \pmod{M}. \qquad (11)$$

Here, introducing a new one-way function $\theta(N)$ of N, g is changed to

$$g_N = g^{\theta(N)} \pmod{n} \qquad (12)$$

and Mt integers $x_\ell^{(N)}$ $(1 \leq \ell \leq t,\ 0 \leq N \leq M-1)$ are selected as

$$\max\{p,q\} \leq x_\ell^{(N)} = y_\ell z_\ell^{(N)} \leq \Phi(n), \qquad (13)$$

where y_ℓ is a measure of $\Phi(n)$, and $z_\ell^{(N)}$ is an integer which satisfies

$\gcd\{z_\ell^{(N)}, \Phi(n)\}=1$. Then the secret information of a user j in the group N_j is given by

$$S_{j\ell}^{(N_j)} = g_{N_j}^{d_j^{(N_j)} x_\ell^{(N_j)}} \pmod n, \quad 1 \le \ell \le t \tag{14}$$

where

$$f_{j\ell} = e_j^\ell \pmod n = \{f(ID_j)\}^\ell \pmod n \tag{15}$$

and

$$d_j^{(N_j)} = \sum_{\ell=1}^{t} x_\ell^{(N_j)} f_{j\ell} \pmod{\Phi(n)}. \tag{16}$$

When a user j in the group N_j wants to get a common-key with a user i in the group N_i, j's secret information $S_{j\ell}^{(N_j)}$ is exchanged with i's secret information by

$$S_{j\ell}^{(N_j N_i)} = \left\{ S_{j\ell}^{(N_j)} \right\}^{\delta_\ell^{(N_i)}} \pmod n, \tag{17}$$

where the exchange information $\delta_\ell^{(N_i)}$ is given by

$$\delta_\ell^{(N_i)} = \frac{\beta\, x_\ell^{(N_i)}\, \mathrm{LCM}\{\theta(N_j), \theta(N_i)\}}{x_\ell^{(N_j)}\, \theta(N_j)} \pmod{\Phi(n)} \tag{18}$$

and β is a random integer, and then the common-key between them is obtained by

$$k_{ji}^{(j)} = \prod_{\ell=1}^{t} \left\{ S_{j\ell}^{(N_j N_i)} \right\}^{f_{i\ell}} \pmod n$$

$$= \prod_{\ell=1}^{t} \left\{ S_{j\ell}^{(N_j)} \right\}^{\delta_\ell^{(N_i)} f_{i\ell}} \pmod n, \tag{19}$$

where the secret informations necessary for the exchange $\{ \delta_\ell^{(N)};\ 1 \le \ell \le t,\ 0 \le N \le M-1 \}$ except $\delta_\ell^{(N^*)}$ for the user's own N^* is calculated by the center and delivered to all users beforehand being accompanied with their own secret information. Following the same process, a user i can obtain the common-key with j by

$$k_{ij}^{(i)} = \prod_{\ell=1}^{t} \left\{ S_{i\ell}^{(N_i N_j)} \right\}^{f_{j\ell}} \pmod n$$

$$= \prod_{\ell=1}^{t} \left\{ S_{i\ell}^{(N_i)} \right\}^{\delta_\ell^{(N_j)} f_{j\ell}} \pmod n. \tag{20}$$

Theorem 4.

$$k_{ij}^{(i)} = k_{ji}^{(j)} = g^{\beta\,\mathrm{LCM}\{\theta(N_i),\theta(N_j)\}\, d_i^{(N_i)}\, d_j^{(N_j)}} \pmod n \qquad (21)$$

Proof: The theorem can be proved by deriving the same expression from $k_{ij}^{(i)}$ and $k_{ji}^{(j)}$ shown by Eqs.(19) and (20).

$$k_{ji}^{(j)} = \prod_{\ell=1}^{t} \left\{ S_{j\ell}^{(N_j)} \right\}^{\delta_\ell^{(N_i)} f_{i\ell}} \pmod n$$

$$= \prod_{\ell=1}^{t} g^{\theta(N_j) d_j^{(N_i)} x_\ell^{(N_j)} \frac{\beta\, x_\ell^{(N_i)}\, \mathrm{LCM}\{\theta(N_j),\theta(N_i)\}}{x_\ell^{(N_j)}\, \theta(N_j)} f_{i\ell}} \pmod n$$

$$= g^{\beta\,\mathrm{LCM}\{\theta(N_j),\theta(N_i)\} d_j^{(N_j)} \sum_{\ell=1}^{t} x_\ell^{(N_i)} f_{i\ell}} \pmod n$$

$$= g^{\beta\,\mathrm{LCM}\{\theta(N_j),\theta(N_i)\} d_j^{(N_j)}\, d_i^{(N_i)}} \pmod n,$$

and

$$k_{ij}^{(i)} = \prod_{\ell=1}^{t} \left\{ S_{i\ell}^{(N_i)} \right\}^{\delta_\ell^{(N_j)} f_{j\ell}} \pmod n$$

$$= \prod_{\ell=1}^{t} g^{\theta(N_i) d_i^{(N_j)} x_\ell^{(N_i)} \frac{\beta\, x_\ell^{(N_j)}\, \mathrm{LCM}\{\theta(N_i),\theta(N_j)\}}{x_\ell^{(N_i)}\, \theta(N_i)} f_{j\ell}} \pmod n$$

$$= g^{\beta\,\mathrm{LCM}\{\theta(N_i),\theta(N_j)\} d_i^{(N_i)} \sum_{\ell=1}^{t} x_\ell^{(N_j)} f_{j\ell}} \pmod n$$

$$= g^{\beta\,\mathrm{LCM}\{\theta(N_i),\theta(N_j)\} d_i^{(N_i)}\, d_j^{(N_j)}} \pmod n.$$

Hence,

$$k_{ij}^{(i)} = k_{ji}^{(j)} = g^{\beta\,\mathrm{LCM}\{\theta(N_i),\theta(N_j)\}\, d_i^{(N_i)}\, d_j^{(N_j)}} \pmod n.$$

(Q.E.D.)

From the above theorem the common-key between two users i and j is given by

$$k_{ij} = g^{\beta\,\mathrm{LCM}\{\theta(N_i),\theta(N_j)\}\, d_i^{(N_i)}\, d_j^{(N_j)}} \pmod n. \qquad (22)$$

Here it is very interesting to consider a special case when M=1 and β=1. The expression of Eq.(22) can be rewritten as

$$k_{ij} = g_0^{d_i^{(0)} d_j^{(0)}} \pmod{n}, \qquad (23)$$

which is equivalent to Eq.(9). Hence the latter scheme is an extension of the former basic system.

VI. Considerations on the Extended System

A) The Number of Necessary Computations

Let us assume that the maximum number of users to join the identiy-based cryptosystem is less than T=Mt and the user's conspiracy must not succeed even when a factorization of n=pq is possible. Then we compare the number of necessary computations to generate a common-key for the basic system with that of the extended system under the condition that the user's memory capacity is equal to T=Mt for the both systems.

For the basic system, t should be increased to T. Then T exponentations mod n and 2(T-1) multiplications mod n are necessary to excute the calculations for Eqs.(4)and (5). On the other hand it is necessary for the extended system only to excute 2t exponentations mod n and 2(t-1) multiplications mod n. Then, as $M \geq 2$, the number of necessary computations for the extended system is much less than that of the basic system, especially when M is large.

B)Existence of $\{x_\ell^{(N_j)}\}^{-1} \pmod{\Phi(n)}$ in Eq.(18)

It is clear that there exists $\{x_\ell^{(N_j)}\}^{-1} \pmod{\Phi(n)}$ if $x^{(N_j)}$ and $\Phi(n)$ are relatively prime, but regretfully, such a condition is not satisfied because $\gcd\{x_\ell^{(N_j)}, \Phi(n)\} = y_\ell$. However, as the numerator of Eq.(18) includes $x_\ell^{(N_j)} = y_\ell z_\ell^{(N_j)}$, the greatest common divisor y_ℓ can be cancelled, and hence, $\{x_\ell^{(N_j)}\}^{-1} \pmod{\Phi(n)}$ exists.

Remark : It is clear that a factor $\theta(N_j)$ of the denominator is a divisor of $\mathrm{LCM}\{\theta(N_i), \theta(N_j)\}$.

C)Probability That the Number of Users in a Group Is Greater Than or Equal to t

In the extended system a group number is specified by $N = \{f(ID)\}^c \pmod{n}$, and if more than or equal to t users belong to a group, the users conspiracy will become possible. Then in order to cope with the possibility, we must consider the probability that the number of users who belong to a specified group N is greater than or equal to t.

Let L be the number of all users in the system, then the probability is given by

$$P_r(L;M,t) = \sum_{i=t}^{L} \binom{L}{i} \left(\frac{1}{M}\right)^i \left(1-\frac{1}{M}\right)^{L-i}, \qquad (24)$$

where M is the number of groups and $\{f(ID)\}^c \pmod M$ is assumed to be a uniformly distributed random number in $[0,M-1]$. Some numerical data are given in Table I.

Table I.

t = 100 M = 100		t = 200 M = 200	
L	Pr(L; M,t)	L	Pr(L; M,t)
1000	6.62×10^{-67}	4000	($< 10^{-100}$)
2000	2.45×10^{-39}	8000	1.31×10^{-74}
3000	2.66×10^{-25}	12000	2.56×10^{-47}
4000	1.14×10^{-16}	16000	1.55×10^{-30}
5000	5.80×10^{-11}	20000	1.75×10^{-19}
6000	4.34×10^{-07}	24000	4.97×10^{-12}
7000	1.83×10^{-04}	28000	4.78×10^{-07}
8000	9.72×10^{-03}	32000	7.53×10^{-04}
9000	1.13×10^{-01}	36000	5.61×10^{-02}

References

[1] A.Shamir, " Identity-based cryptosystems and signature schemes," Proceedings of CRYPTO'84, Lecture Notes in Computer Science 196, Springer Verlarg, 1985.

[2] A.Shamir,"How to share a secret," Comm. ACM, vol.22, No.11, Nov. 1979.

[3] R.J.McEliece and D.V.Sarwate, "On sharing secrets and Reed-Solomon codes," Comm. ACM, vol.24, No.9, Sept. 1981.

[4] Data Encryption Standard. Federal Information Processing Standards (IFIPS) Publication No.46, National Bureau of Standards, January 1977.

[5] S.Miyaguchi,"Criteria for the strength of encipherment and standardization for cryptographic techniques," Proceedings of the 1986 Symposium on Cryptography and Information Security, Feb. 1986.