Key Distribution Systems Based on Identification Information

Eiji OKAMOTO

Information Basic Research Laboratory
C&C Information Technology Research Laboratories
NEC Corporation
4-1-1 Miyazaki, Miyamae-ku
Kawasaki, Kanagawa, 213, Japan
Telephone: +81-44-855-1111, Ext. 3631

ABSTRACT

Two types of key distribution systems based on identification information are proposed, one for decentralized networks and the other for centralized networks. The system suitable for decentralized networks is analogous to the Diffie-Hellman public key distribution system, in which the former uses each user's identification information instead of a public file used in the latter. The proposed system is able to defend the networks from impostors. The system suitable for centralized networks, which is less analogous to the Diffie-Hellman system, can also defend the networks from impostors, though the network center does not have any directory of public or private key-encrypting keys of the users. Both of the systems proposed in this paper do not require any services of a center to distribute work keys, or users to keep directories of key-encrypting keys. Therefore, key management in cryptosystems can be practical and simplified by adopting the identity-based key distribution systems.

1. Introduction

Diffie and Hellman first proposed the idea of the public key distribution system in which two users, knowing only public information, could establish a secret key for conventional cryptosystems[1]. However, in order to establish a correct key, it requires an authenticated file of user's public information.

This paper proposes two types of key distribution systems based on

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 194-202, 1988.

identification information, one for decentralized networks[2] and the other for centralized networks. The system suitable for decentralized networks is analogous to the Diffie-Hellman public key distribution system, in which the former uses each user's identification information instead of a public file used in the latter. Any information such as one's name and address can be used as the identity information if it is known to everybody and uniquely identifies the user. The proposed system is able to defend the networks from impostors. The system suitable for centralized networks, which is less analogous to the Diffie-Hellman system, can also defend the networks from impostors, though the only network center uses the identification information. Both of the systems proposed in this paper do not require any services of a center to distribute work keys, or users to keep directories of key-encrypting keys.

The identity-based key distribution systems assume the existence of a trusted card issuer. The only purpose of the center is to give each user a personalized IC card, when the network is initially set up or a new user joins the network. Even when a new user joins, previously delivered cards to other users need not be updated.

The advantages of applying identification information to cryptosystems have been already shown by Shamir at Crypto'84[3]. We applied his idea to the Diffie-Hellman public key distribution system to eliminate the public file.

Key distribution systems using the public key certificates[4], which are user's public keys signed by a central authority, have almost same advantages. However, the identity-based key distribution systems are simpler than the certificate systems whatever public key cryptosystem is used for the certificates. When RSA public key cryptosystem[5] is used, all certificates must have different modulus n[6], whereas the modulus n in the proposed systems is a constant. Since no other public key cryptosystems have simpler form than RSA, the proposed systems are considered to be more practical than the certificate systems.

2. The Principle of Identity-based Key Distribution Systems

The identity-based key distribution systems have two phases: card issue phase and key generation phase. On the request of a new user, the card issuer gives him his card if he is confirmed. Each user

with his own IC card can generate a work key through the protocols below. The IC cards should not be rewritten but by the card issuer.

2.1 The System Suitable for Decentralized Networks

In decentralized networks, there are no network centers, and each user communicates with other users directly. In these networks, the card issuer generates two prime numbers p and q about 256 bits long, and determines numbers e and d, satisfying

$$e \cdot d (\mathrm{mod} (p-1) \cdot (q-1)) = 1, \tag{1}$$

with both e and d less than $n=p \cdot q$. It also determines an integer g which is a primitive element in GF(p) and GF(q). For user i whose identification information is IDi, the center calculates an integer si:

$$si = IDi^{-d} \pmod{n}, \tag{2}$$

and stores the set of integers (n,g,e,si) in his IC card, and gives it to him. Number d can be aborted after all the cards are distributed. If there are no new users expected, even the center can be closed. Hence, d is kept secret from any user, si is known only to user i and n,g,e are common to all the users. Figure 1 (a) illustrates the card issue phase.

When users i and j wish to obtain a work key between themselves, user i generates a random number ri and sends user j the integer xi:

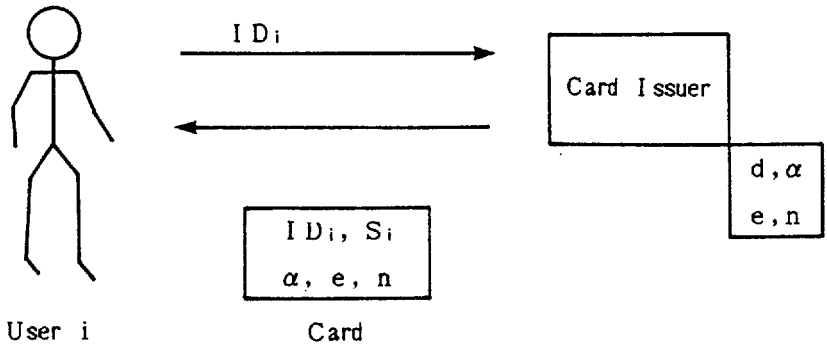
$$xi = si \cdot g^{ri} \pmod{n}. \tag{3}$$

User j also generates a random number rj and sends user i the integer xj:

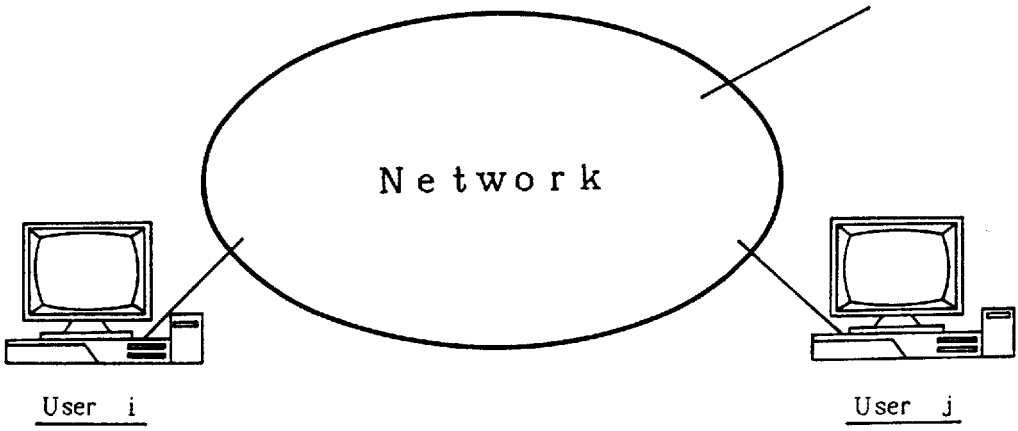
$$xj = sj \cdot g^{rj} \pmod{n}. \tag{4}$$

Then, users i and j compute work keys WKi,WKj respectively as follows:

$$WKi = (xj^{e} \cdot IDj)^{ri} \pmod{n} \tag{5}$$



(a) Card Issue Phase



Random Number ri
$xi = Si \cdot \alpha^{ri} \pmod n$
$wki = (xj^e \cdot IDj)^{ri} \pmod n$

Random Number rj
$xj = Sj \cdot \alpha^{rj} \pmod n$
$wkj = (xi^e \cdot IDi)^{rj} \pmod n$

(b) Key Generation Phase

Fig. 1. Identity-based Key Distribution System
(Decentralized Network)

$$WKj=(xi^{e}\cdot IDi)^{rj} \pmod{n}. \quad (6)$$

Both work keys turn out to be equal, because

$$WKi=WKj=g^{e\cdot ri\cdot rj} \pmod{n}. \quad (7)$$

Figure 1 (b) shows the key generation phase.

2.2 The System Suitable for Centralized Networks

In centralized networks, each user can communicate with other users only via a network center. In these networks, the card issuer gives (n,e,r) to the network center, and distributes each IC card storing (n,g,y,si) to user i, where n,g and si have the same properties as in 2.1, r is any fixed integer less than n, and y is

$$y=g^{e\cdot r} \pmod{n}. \quad (8)$$

Figure 2 (a) illustrates the card issue phase.

When user i wishes to generate a work key between him and the network center, he generates a random number ri and sends xi satisfying

$$xi=si\cdot g^{ri} \pmod{n} \quad (9)$$

to the network center. The work key WKi is given by

$$WKi=y^{ri} \pmod{n}. \quad (10)$$

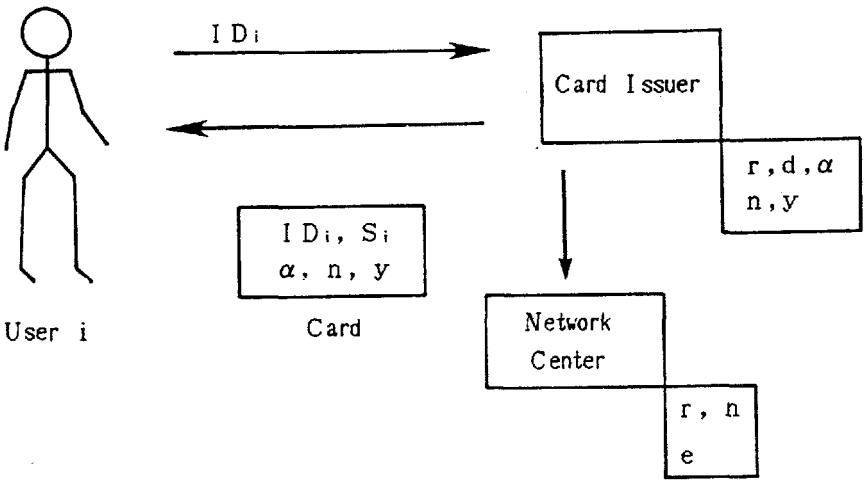
Receiving xi from user i, the center calculates the work key WK as follows:

$$WK=(xi^{e}\cdot IDi)^{r} \pmod{n}. \quad (11)$$

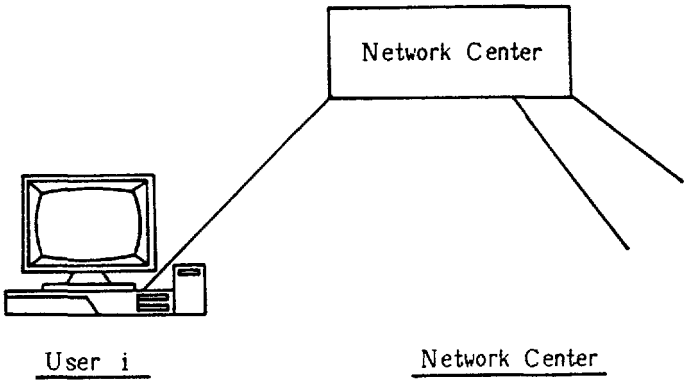
Both work keys WKi and WK are equal to

$$WKi=WK=g^{e\cdot ri\cdot r} \pmod{n}. \quad (12)$$

Figure 2 shows the key generation phase.



(a) Card Issue Phase



Random Number r_i

$x_i = S_i \cdot \alpha^{r_i} \pmod n$

$w_{ki} = y^{r_i} \pmod n$

$\rightarrow w_k = (x_i^e \cdot ID_i)^r \pmod n$

(b) Key Generation Phase

Fig. 2. Identity-based Key Distribution System (Centralized Network)

3. Security of the Identity-based Key Distribution Systems

The security of the systems depend on the difficulty of finding x and r satisfying

$$IDk \cdot x^e = g^{e \cdot r} \pmod{n} \tag{13}$$

for some k. If found, one can send the integer x to any user of the decentralized networks or the network center of the centralized network, disguising himself as user k. Finding x in Eq.(13) with r given is equivalent to decrypting RSA cryptosystems without decryption keys. Calculation of r in Eq.(13) with x given becomes the discrete logarithm computation.

Assume there were i and j such that

$$IDk = IDi^a \cdot IDj^b \pmod{n} \tag{14}$$

for some integers a and b. Then, user i and j can succeed to satisfy Eq.(13) together, with x and r given by

$$x = xi^a \cdot xj^b \pmod{n} \tag{15}$$

$$r = a \cdot ri + b \cdot rj. \tag{16}$$

However, the probability of the existence of a and b satisfying Eq.(14) can be made small, by introducing redundancy to each ID or applying a hash function to them. Even if the number of ID's in use is one trillion, the ratio of ID to the number less than n is $10^{12}/2^{512} = 10^{-142}$.

4. Applications

The identity-based key distribution system for decentralized networks is applicable to any bidirectional real-time communication networks. Telephone is a typical example. Recently almost all personal computer networks have real-time "talk" services which the proposed system can be applied to.

The centralized type system is applicable to any networks with a network center---for example, an electronic mail system, a data base

system, and so on.

When these networks adopt the identity-based key distribution system, the most time-consuming operation is the exponentiation:

$$y=x^e \pmod n. \qquad (17)$$

Recently, chips that can compute exponentiation in o.1 second are available. Even the chips for digital signal processing can calculate it within a second. The NEC DSP-77230 took 0.7 second. Hence the calculation of the identity-based key distribution systems do not require a big amount of time.

5. Concluding Remarks

Two types of identity-based key distribution system have been proposed for decentralized networks and centralized networks. The latter system requires only one way communication to establish a common work key. This is because it does not use the identification information of the network center. In the centralized networks, however, there have been proposed lots of key distribution systems so far. We have showed that the identity-based key distribution system does not need any public or private key-encrypting key list in the network center.

In this proposal, each system uses a common modulus n, though RSA cryptosystem cannot[6]. Moreover, the work keys are randomly determined. In the Diffie-Hellman public key distribution system, work keys between two fixed users are always a constant.

Acknowledgments

I would like to thank Masao Managaki, Katsuhiro Nakamura and Kazue Tanaka of NEC Corporation for helpful suggestions and discussions.

References

[1] DIFFIE,W., and HELLMAN,M.E.:"New directions in cryptography,"IEEE Trans., IT-22, pp.644-654, 1976.

[2] OKAMOTO,E.:"Proposal for identity-based key distribution systems," Electronics Letters, 22, pp.1283-1284, 1986.

[3] SHAMIR,A.:"Identity-based cryptosystems and signature schemes," Proc. Crypto 84, Santa Barbara, August 1984, pp.47-53.

[4] KOHNFELDER,L.:"Towards a practical public-key cryptosystem," B.S. Thesis, M.I.T., Cambridge, Mass.

[5] RIVEST,R.L., SHAMIR,A., and ADLEMAN,L.:"A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, 21, pp.120-126, 1978.

[6] SIMMONS,G.J.:"A 'weak' privacy protocol using the RSA crypto algorithm," Cryptologia, 7, pp.180-182, 1983.