Security Certified Identity-Based Non-Interactive Key Sharing

Hatsukazu Tanaka
Department of Electrical & Electronics Engineering
Faculty of Engineering, Kobe University
Rokko, Nada, Kobe, 657 Japan

Abstract In this paper a new identity-based non-interactive key sharing (IDNIKS) scheme has been proposed. The Algorithm is very simple and hence easily implemented. The security depends on the difficulty of factoring, and it seems to be very secure for user's collusion.

I. Introduction

At the Crypto'84 Shamir[1]has proposed a new concept of identity-based cryptosystems and signature schemes. The new concept is much attractive and has stimulated many cryptographic researchers to realize it. Several realization schemes have been proposed, but regretfully they are insecure for user's collusion. Recently Maurer and Yacobi [2] has proposed a secure realization scheme for user's collusion, but it is extremely difficult to implement.

In this paper a new identity-based non-interactive key sharing scheme (IDNIKS) has been proposed in order to realize the original concept of identity-based cryptosystem. The algorithm is very simple and easily imple-mented. The security depends on the difficulty of factoring, and it seems to be very secure for user's collusion.

II. Basic Center Algorithm

Let P and Q be two large primes and their product be N=PQ. Then the Carmichael function of N can be given by L = LCM { P-1,Q-1}. Let g be a primitive element over GF(P) and GF(Q), and let denote each user's public identity information with $ID_\ell(\ell=A,B,C,....)$. Here we introduce three integers e, e_1 and e_2 which satisfy $\gcd\{e_1,e_2\}=1$, $\gcd\{e_1,e\}=1$, and ee_2-e_1 is large enough, and a one-way hash function f to calculate two hashed identity informations

$$I_{\ell 1} = e_1 f(ID_\ell) + e \qquad (1)$$

and

$$I_{\ell 2} = e_2 f(ID_\ell) + 1. \qquad (2)$$

Then we introduce two random numbers r_1 and r_2, and a user ℓ's proper random number r_ℓ ,and calculate the following equations.

$$g_{\ell 1} = r_\ell^{-d} \cdot g^{xI_{\ell 1}^2} \pmod N \qquad (3)$$

$$g_{\ell 2} = r_\ell^{e^2 d} \cdot g^{yI_{\ell 2}^2} \pmod N \qquad (4)$$

where

$$x = \frac{r_1 L}{\gcd\{ e_1^2(ee_2+e_1)r_1,\ L \}} \qquad (5)$$

$$y = \frac{r_2 L}{\gcd\{ e_2^2(ee_2+e_1)r_2,\ L \}} \qquad (6)$$

and

$$d = \frac{L}{\gcd\{ ee_2-e_1,\ L \}} \qquad (7)$$

Here remark that $xe_1^{\ 2}(ee_2+e_1)=0 \pmod L$, $ye_2^{\ 2}(ee_2+e_1)=0 \pmod L$ and $(ee_2-e_1)d = 0 \pmod L$. Finally the trusted center publishes $\{N,f,e,e_1,e_2\}$ and delivers$\{g_{\ell 1},g_{\ell 2}\}$to each user ℓ through a secure channel or by an IC card.

III. Non-Interactive Key Sharing

We assume here that two users A and B want to share a common-key K_{AB} between them non-interactively. First A calculates B's hashed identity informations I_{B1} and I_{B2} from ID_B using the one-way hash function f, and then performs the following simple calculation to share a common-key K_{AB}.

$$K_{AB}^{(A)} = g_{A1}^{I_{B1}^2} \cdot g_{A2}^{I_{B2}^2} \pmod N$$

$$= g^{xI_{A1}^2 I_{B1}^2 + yI_{A2}^2 I_{B2}^2} \pmod N \qquad (8)$$

Similarly, B obtains $K_{AB}^{(B)} = K_{AB}^{(A)}$. Hence their common-key is given by

$$K_{AB} = g^{xI_{A1}^2 I_{B1}^2 + yI_{A2}^2 I_{B2}^2} \pmod N. \qquad (9)$$

IV. Security

The most successful attack to the proposed IDNIKS is considered to forge a common-key between the third parties by disclosing the center's secrets $g^x \pmod N$ and $g^y \pmod N$ using the public informations and the simultaneous equations derived by the user's collusion. However, we can solve only on $g^{x(ee_2-e_1)} \pmod N$ and $g^{y(ee_2-e_1)} \pmod N$ even if many users collude. Then it is necessary for us to obtain the inverse element of (ee_2-e_1) under the condition that the modulus L is unknown in order to perform the attack shown above. This is the same situation as the case of RSA public-key cryptosystem. Hence the security of this IDNIKS clearly depends on the difficulty of factoring a composite number N of two large primes P and Q.

V. Conclusion

In this paper a new realization scheme of IDNIKS has been proposed. The algorithm is very simple and easily implemented. The security depends on the difficulty of factoring, and the proposed IDNIKS can be certified to be secure against the attacks involving user's collusion.

References

[1] A.Shamir,"Identity-based cryptosystems and signature schemes",Proceedings of Crypto'84, pp.47-53, 1985.

[2] U.M.Maurer and Y.Yacobi, " Non-Interactive public-key cryptosystem", Proceedings of Eurocrypt'91, pp.498-507, 1991.

0 - 7803-2015-8/94/$4.00 ©1994 IEEE