Secure Conference Key Distribution Schemes for Conspiracy Attack

Kenji Koyama

NTT Communication Science Laboratories
Seika-cho, Soraku-gun, Kyoto 619-02 Japan

Abstract

At the Eurocrypt'88 meeting, we proposed three identity-based conference key distribution schemes. At the Asiacrypt'91 meeting, Shimbo and Kawamura presented a conspiracy attacking method which worked against our schemes to disclose a user's secret information. This paper proposes an improved identity-based conference key distribution scheme to counter this attack.

1. Introduction

Since Diffie and Hellman proposed the public key distribution system (DH scheme), several advanced schemes and problems related to the DH scheme have been presented [ITT82, S85, O86, KO87, Y87, KO88, M88, LLH89, Y90, FM90, CI90]. One direction which the advanced schemes have taken is to authenticate exchanged messages with each user's identification information. This is called an identity-based system. Another direction being taken is to generate a common key among two or more users called a conference key. Several conference key distribution schemes have previously been presented [ITT82. KO88, LLH89, CI90]. These schemes can be regarded as examples of general multiparty protocols [B91, MR91], in which each of m members in a network has a private input x_i. Together, the members would like to compute, *correctly*, *privately* and *fairly*, any computable function $F(x_1, \cdots, x_m)$. In particular, multiparty protocols must be robust (secure) to guard against cheating members.

At the Eurocrypt'88 meeting, we proposed three identity-based conference key distribution schemes, constructed for star, complete graph and ring networks [KO88]. At the Asiacrypt'91 meeting, Shimbo and Kawamura presented a method for attacking our schemes for star and complete graph networks [SK91]. They pointed out that a pivot user's secret information could be revealed by a conspiracy between two legal users' conspiracy by using the Euclidean algorithm. In order to counter their attack, we propose improving the identity-based conference key distribution schemes by introducing new random variables.

2. Improved Conference Key Distribution Schemes

All identity-based conference key distribution schemes consist of a center procedure and a user procedure as follows.

[Center Procedure]

A trusted center generates the following information:

- Three large primes (p, q, r) and the partial product $N = pq$.
- Integers (e, d) satisfying the congruence:

$$ed \equiv 1 \bmod L, \quad \text{where } L = \text{lcm}(p-1, q-1, r-1).$$

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 449-453, 1993.

- An integer g which is a primitive element over GF(p), GF(q) and GF(r).
- An integer S_i which is derived from user i's identification information I_i as follows:

$$S_i = I_i^d \bmod Nr, \qquad I_i = h(ID_i),$$

where ID_i is user i's original identifier, and h is a public one-way hash function.

The above information is classified into three categories: a secret system key (p, q, d), a public system key (N, r, g, e), and a secret user key S_i for user i.

[User Procedure]

Let m be the number of users in a group sharing a common conference key. For simplicity, a user procedure for a star network is described here. One user becomes a "pivot user", who communicates with the other $(m - 1)$ users belonging to the group. The procedures for interactions between the pivot user, user 1, and one of the other users, user j $(2 \leq j \leq m)$ are summarized as follows.

Step 1: User j's procedure.

Step 1.1 Choose a random number P_j and compute its reciprocal $\overline{P}_j$:

$$P_j\overline{P}_j \equiv 1 \pmod{(r-1)}$$

Step 1.2 Compute the following (X_j, Y_j):

$$X_j = g^{eP_j} \bmod Nr,$$

$$Y_j = S_j g^{h(X_j \| Time)P_j} \bmod Nr.$$

Step 1.3 Send $(I_j, X_j, Y_j, Time)$ to user 1.

Step 2: User 1's procedure.

Step 2.1 Check the time and whether the following congruence holds:

$$Y_j^e / X_j^{h(X_j \| Time)} \equiv I_j \pmod{Nr}.$$

If the congruence holds, user 1 is able to verify that the message is from user j.

Step 2.2 Choose random numbers R_1 $(0 < R_1 < r)$ and Q_{1j} $(0 < Q_{1j} < N,\ 2 \leq j \leq m)$.

Step 2.3 Compute the following (A_{1j}, B_{1j}):

$$A_{1j} = (X_j + Q_{1j}r)^{eR_1} \bmod Nr,$$

$$B_{1j} = S_1(X_j + Q_{1j}r)^{h(A_{1j} \| Time)R_1} \bmod Nr.$$

Step 2.4 Send $(I_1, A_{1j}, B_{1j}, Time)$ to user j.

Step 2.5 Compute the common key K with

$$K = g^{e^2 R_1} \bmod r.$$

Step 3 User j 's procedure.

Step 3.1 Check the time and whether the following congruence holds:

$$B_{1j}^{e}/A_{1j}^{h(A_{1j}\|Time)} \equiv I_1 \pmod{Nr}.$$

If the congruence holds, user j is able to verify that the message is from user 1.

Step 3.2 Compute the common key K with

$$\begin{aligned} K &= A_{1j}^{\overline{P}_j} \bmod r \\ &= g^{e^2 R_1} \bmod r. \end{aligned}$$

Remarks:

1. The term $(X_j + Q_{1j}r)$ in variables A_{1j} and B_{1j} in this new version was represented by the term X_j in the previous version [KO88]. This improvement renders Shimbo and Kawamura's attack ineffective. The details will be discussed in Section 4.

2. The exponents $h(X_j\|Time)$ and $h(A_{1j}\|Time)$ in this new version were previously represented by the exponents X_j and A_{1j}, respectively, where $\|$ denotes concatenation. The usage of a time stamp with a public one-way hash function h is effective in preventing a replay attack.

3. Shimbo and Kawamura's Attacking Method

Here, a brief description is given of Shimbo and Kawamura's attacking method [SK91] for the previous version where the term X_j was used instead of the terms $(X_j + Q_{1j}r)$ in the variables A_{1j} and B_{1j}. Their attack requires a conspiracy between two users, other than user 1, belonging to the group. The attackers' aim is to disclose the pivot user's secret information S_1. Note that if this attack succeeds, the attackers can pretend to be user 1 in the subsequent key generation procedure. A concrete attacking procedure is as follows. Assume that user 2 and user 3 conspire and user 2 becomes a "pivot conspirator". First, user 3 sends (P_3, A_{13}, B_{13}) to user 2. Next, user 2 computes T:

$$\begin{aligned} T &= B_{12}^{P_3 A_{13}}/B_{13}^{P_2 A_{12}} \bmod Nr \\ &= S_1^{P_3 A_{13} - P_2 A_{12}} \bmod Nr. \end{aligned}$$

Since user 2 knows the value of the exponent $(P_3 A_{13} - P_2 A_{12})$, denoted by c, and the relation:

$$S_1^e \equiv I_1 \bmod Nr,$$

the "Euclidean Attack" [SS3] can be applied as follows: if e and c are coprime, the integer solution (x, y) satisfying $ex + cy = 1$ can be easily obtained by the Euclidean algorithm. Then, S_1 is derived from (I_1, T, x, y) with

$$\begin{aligned} I_1^x T^y \bmod Nr &= S_1^{ex+cy} \bmod Nr \\ &= S_1 \bmod Nr. \end{aligned}$$

Finally, user 2 sends S_1 to user 3.

The probability of a successful attack being carried out can be estimated by the probability that e and c are coprime. If P_1 and P_2 are chosen as a coprime pair and $e = 3$, then the probability of a successful attack is about 0.67.

It should be noted that this conspiracy attacking method is vulnerable because the non-pivot conspirator (user 3) discloses his secret information P_3. Once user 2 obtains the value of P_3, he can easily compute the value of S_3 with

$$S_3 = Y_3/g^{X_3P_3} \bmod Nr.$$

Thus, the conspiracy attack is based on maintaining "trust" between the conspirators.

4. Security of New Schemes

The security of the improved schemes is based on the difficulty of deriving secret information from public keys, transmitted messages and the other user's secret keys. The secrecy of (p, q, d) is based on the difficulty of factoring a large number N, while the secrecy of $(P_i, \overline{P}_i, R_i, K, K')$ is based on the difficulty of computing a discrete logarithm over $GF(r)$. In the new version, the secrecy of S_i is based on the difficulty of computing P_i or extracting the e-th roots mod N when the factors of N are unknown.

As pointed out in [SK91], the previous version was attacked because only the fixed common random number R_1 was used to compute A_{1j} and B_{1j} $(2 \leq j \leq m)$ for each user. As a result, S_1^Z mod Nr with a known integer Z $(\neq e)$ could easily be computed by canceling the random number R_1 through the conspiracy of two users.

An effective means of countering this attack is to introduce distinct random numbers Q_{1j} $(2 \leq j \leq m)$ into old variables (A_{1j}, B_{1j}). It is clear that new variables (A_{1j}, B_{1j}) satisfy the completeness properties which are needed to authenticate user 1's identity and to generate a common conference key. Even if the conspirators compute the variables $T = B_{12}^{P_3A_{13}}/B_{13}^{P_2A_{12}}$ mod Nr for the new version, T cannot be expressed by S_1^Z mod Nr with a known integer Z $(\neq e)$.

Our proposed new schemes can be regarded as variants of the parallel version of the extended Fiat-Shamir scheme [FS86,FFS87,OO88,GQ88]. Although the value of $(X_j + Q_{1j}r)$ mod r is known by user j, the value of $(X_{1j} + Q_{1j}r)$ mod N is random and unknown to user j $(j \neq 1)$. Thus, the transmitted messages B_{1j} are independent of the secret S_1 and there are no additional information leaks about S_i in our schemes. Formally speaking, the parallel version of the extended Fiat-Shamir is a non-transferable (weak zero-knowledge) interactive proof system [OO88,GQ88]. Thus, we have the following lemma.

Lemma (Non Transferability) *In the new version of the identity-based conference key distribution schemes, no transferable information about a secret S_i is revealed.*

5. Conclusion

Improved interactive conference key distribution schemes were proposed to counter Shimbo and Kawamura's conspiracy attack. The introduction of new random variables was shown to be effective in preventing the disclosure of a user's secret key in the interactive protocols. The new schemes require additional time for the generation of $(m - 1)$ random variables and $(m - 1)$ additions modulo Nr. The transmission efficiency of the new schemes is the same as that of the previous schemes.

Acknowledgements

We wish to thank Kazuo Ohta (presently at MIT) and Michael Wang (University College, U.N.S.W.) for their valuable comments.

References

[B91] D. Beaver: "Foundations of Secure Interactive Computing", Proc. of CRYPTO'91, pp.9-1–9-7 (1991).

[CI90] T. Chikazawa and T. Inoue: "A new key sharing system for global telecommunications", Proc. of GLOBCOM'90, pp.1069-1072 (1990).

[FM90] W. Fumy and M. Munzert: "A modular approach to key distribution", Proc. of CRYPTO'90, pp.274-283 (1990).

[FS86] A. Fiat and A. Shamir: "How to prove yourself: Practical solutions to identification and signature problems", Proc. of CRYPTO'86, pp.186-194 (1986).

[FFS87] U. Feige, A. Fiat and A. Shamir: "Zero knowledge proofs of identity", Proc. of STOC, pp.210-217 (1987).

[GQ88] L.C. Guillou and J. J. Quisquarter: "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory", Proc. of Eurocrypt'88, pp.123-128 (1990).

[ITT82] I. Ingemarson, D.T. Tang and C.K. Wong: "A conference key distribution system", IEEE Trans. on Information Theory, Vol. IT-28, pp.714-720, (1982).

[KO88] K. Koyama and K. Ohta: "Security of Improved Identity-based Conference Key Distribution Systems", Proc. of Eurocrypt'88, pp.11-19 (1989).

[LLH89] C.S. Laih, J.Y. Lee and L. Harn: "A new threshold scheme and its application in designing the conference key distribution cryptosystem", Information Processing Letters, Vol.32, No.3, pp.95-99 (1989).

[M88] K.S. McCurley: "A key distribution system equivalent to factoring", J. of Cryptology, Vol.1 , No. 2, pp.95-106, (1988).

[MR91] S. Micali and P. Rogaway: "Secure computation", Proc. of CRYPTO'91, p9-8 (1991).

[O86] E. Okamoto: "Proposal for identity-based key distribution systems", Electronics Letters Vol.22 pp.1283-1284 (1986).

[OO88] K. Ohta and T. Okamoto: "A modification of the Fiat-Shamir scheme", Proc. of CRYPTO'88, pp.232-243 (1988).

[S83] G. J. Simmons: "A 'weak' privacy protocol using the RSA crypto algorithm", Cryptologia 7, 2, pp.180-182 (1983).

[S85] Z. Shmuely: "Composite Diffie-Hellman public-key generating systems are hard to break", TR. NO. 356, Computer Science Dept. Technion, IIT, Feb. (1985).

[SK91] A. Simbo and S. Kawamura "Cryptanalysis of several conference key distribution schemes", Proc. of Asiacrypt'91, pp.155-160 (1991).

[Y90] Y. Yacobi: "A key distribution "paradox"", Proc. of CRYPTO'90, pp.268-273 (1990).