AN ATTACK ON SUN ET AL.'S GROUP SIGNATURE SCHEME

Hwang, Shin-Jia, Shi, Chi-Hwai, and Huang, Yu-Hui*
Department of Information Management, Chaoyang University of Technology
Wufeng, Taichung Country, 413, Taiwan, R.O.C.
*Department of Computer Science, National Chung Hsing University
250, Kuo Kuang Road, Taichung, 402, Taiwan, R.O.C.
Email: sjhwang@mail.cyut.edu.tw
*Email: chshi@cs.nchu.edu.tw

Abstract

Lee and Chang proposed an efficient group signature scheme but their scheme does not provide unlinkability properties. To improve Lee and Chang's scheme, Sun et al. proposed another group signature scheme. In this paper, an attack is proposed to show that Sun et al.'s scheme does not satisfy unlinkability properties. Moreover, Sun et al.'s scheme does not satisfy anonymity property.

Keywords: Group signature scheme, digital signature.

1. INTRODUCTION

Chaum and van Heyst proposed the concept of group signature scheme [1]. In [1], a group signature scheme must satisfy three basic properties: Authorization. Anonymity, and revocability properties. The authorization property means that only the group member can generate group signatures. The anonymity property means that a receiver cannot identify the anonymous signer during the verification process of group signatures. The revocability property means that, in case of disputes, the anonymous signer of group signatures can be identified with the help of the group manager. Lee and Chang [2] proposed their efficient group signature scheme satisfying these three properties.

For a group signature scheme, Petersen [3] gave four additional properties: Unforgeability, unlinkability, no framing, and efficient properties. The unforgeability property means that no unauthorized user can forge valid group signatures. According to the unlinkability property, it is impossible to determine whether or not two group signatures are generated by the same member. The no framing property means that a group member cannot be falsely accused of some group signatures that he did not generate by a coalition of group members or the group manager. The efficient property means that both the group signature generation and verification do not need the help of the group manager.

Sun et al. point out that Lee and Chang's scheme does not satisfy the unlinkability property. To improve Lee and Chang's scheme, they proposed their new group signature scheme. They claimed that their scheme is better than Lee and Chang's scheme since their scheme satisfies the unlinkability property. Moreover, even the signers of group signatures are identified, these signers does not need to change their certificates from the group manager.

Here, an attack on Sun et al.'s scheme is proposed to show that Sun et al.'s scheme does not satisfy not only the unlinkability property but also the anonymity property. In the following section, the review of Sun et al.'s group signature scheme is given. The attack on Sun et al.'s scheme is given in Section 3. Finally, Section 4 is our conclusions.

2. REVIEW OF SUN ET AL.'S GROUP SIGNATURE SCHEME

Sun et al.'s group signature scheme contains five phases: the Initiation Phase, the Registration Phase, the Signature Phase, the Verification Phase, and the Arbitration Phase.

[Initiation Phase]

Suppose that U_T is a group manager. He selects a large prime number p such that $p= 4p'\times q'+1$, where p' and q' are two large prime numbers. Then he computes $q= p'\times q'$. The parameter $g\in Z^*_p$ is a generator with order q and the function h() is a one-way hash function. Let each user U_i have his private key $x_i\in Z^*_q$ and his public key $y_i= g^{x_i} \bmod p$. Finally, p, q, g, and h() are public while p' and q' are secret.

[Registration Phase]

Suppose that a user U_i wants to join a group. For the new member U_i, the manager U_T randomly finds an integer $k_i\in Z^*_q$ satisfying the following two requirements:

(1) The value $r_i= g^{-k_i}y_i^{k_i} \bmod p$ is not used for the other group members.

(2) There is a solution s_i for the equation $s_i^2+1\equiv k_i-r_ix_T \pmod q$.

Finally, U_T stores (ID_i, r_i, s_i) in his local secret table and sends (r_i, s_i) to U_i, where ID_i is the unique identity of the user U_i. After receiving (r_i, s_i) from U_T, U_i verifies the correctness (r_i, s_i) by the equation $r_i\equiv (g^{s_i^2+1}y_T^{r_i})^{x_i-1} \pmod p$.

[Digital signature phase]

To generate the group signature for a message m, the user U_i selects two random numbers a_1 and $a_2\in Z^*_p$. Then he computes r_i', r_i'', s_i', d_1, d_2, d_3, r, and s by the following steps.

Step 1: Compute $r_i'= r_i^{a_1} \bmod p$ and $s_i'= a_2s_i \bmod q$.

Step 2: Find b satisfying $b(s_i^2+1)\equiv (s_i')^2+1 \pmod q$.

Step 3: Compute $c= b/a_1 \bmod q$ and $d_1= br_i/r_i' \bmod q$.

Step 4: Select a random number a_3 and compute $d_2= (r_i')^{a_3} \bmod p$.

Step 5: Compute $r_i''= (r_i')^c \bmod p$.

Step 6: Find d_3 satisfying $(r_i')^2+(r_i'')^2+1\equiv cd_2+a_3d_3 \pmod q$.

Step 7: Select a random number t and then compute $\alpha_i'= g^{(s_i')^2+1}y_T^{d_1r_i'}$ mod p and $r= (\alpha_i')^t \bmod p$.

Step 8: Find s satisfying $h(m)\equiv rx_i+ts \pmod q$.

Finally, he sends $(m, r_i', r_i'', s_i', d_1, d_2, d_3, r, s)$ to the receiver, where $(r_i', r_i'', s_i', d_1, d_2, d_3, r, s)$ is the group signature for the message m.

[Verification phase]

After receiving $(m, r_i', r_i'', s_i', d_1, d_2, d_3, r, s)$ from U_i, the receiver verifies it by the following steps.

<u>Step 1:</u> Compute $\alpha'_i = g^{(s_i')^2+1} y_T^{d_1 r_i'}$ mod p.

<u>Step 2:</u> Compute $DH_i = \alpha_i' r_i''$ mod p.

<u>Step 3:</u> Check the correctness of the equations $(r_i')^{(r_i')^2+(r_i'')^2+1} \equiv (r_i'')^{d_2} d_2^{d_3}$ (mod p) and $(\alpha_i')^{h(m)} \equiv r^s DH_i^r$ (mod p). If the equations hold, then he accepts the group signature of the message m.

[Arbitration phase]

After receiving $(m, r_i', r_i'', s_i', d_1, d_2, d_3, r, s)$ from some receiver, the group manager U_T first check the correctness of $(m, r_i', r_i'', s_i', d_1, d_2, d_3, r, s)$ by checking $(r_i')^{(r_i')^2+(r_i'')^2+1} \equiv (r_i'')^{d_2} d_2^{d_3}$ (mod p) and $(\alpha_i')^{h(m)} \equiv r^s DH_i^r$ (mod p). If the equations hold, then U_T accepts $(m, r_i', r_i'', s_i', d_1, d_2, d_3, r, s)$. Now he wants to find out the signer of $(m, r_i', r_i'', s_i', d_1, d_2, d_3, r, s)$. For each member U_i with (r_i, s_i) in the group, the manager U_T computes $b = [((s_i')^2+1)/(s_i^2+1)]$ mod q and $\beta = (d_1 r_i'/b)$ mod q. If $\beta \equiv r_i$, then U_i is the signer. Because $r_i \equiv (d_1 r_i'/b) \equiv (b r_i/r_i')(r_i'/b)$ (mod q), the group manager can determine who is the signer.

3. AN ATTACK ON SUN ET AL.'S SCHEME

In this section, an attack is proposed to show that Sun et al.'s scheme does not provide the anonymity and unlinkability properties. Suppose that the receiver asks the group manager to identify the signer of $(m_1, r_{i1}', r_{i1}'', s_{i1}', d_{11}, d_{21}, d_{31}, r_1, s_1)$. The group manager can identify the anonymous signer as the user U_i. Then the receiver computes

$$b_1 = [((s_{i1}')^2+1)/(s_i^2+1)] \text{ mod } q, \text{ and}$$

$$r_i/(s_i^2+1) = r_{i1}/(s_{i1}^2+1) \text{ mod } q = [(d_{11} r_{i1}')/((s_{i1}')^2+1)] \text{ mod } q.$$

The reason why $r_i/(s_i^2+1) = r_{i1}/(s_{i1}^2+1)$ mod $q = [(d_{11} r_{i1}')/((s_{i1}')^2+1)]$ mod q is given below.

$$r_i \equiv r_{i1} \equiv (d_{11} r_{i1}'/b_1) \equiv (d_{11} r_{i1}'(s_i^2+1)/((s_{i1}')^2+1)) \pmod q$$

Since each group member has distinct (r_i, s_i), the value $r_i/(s_i^2+1)$ can be used as the unique pseudonym of the user U_i in the group. To determine whether or not the user U_i is the signer of another new $(m_2, r_{i2}', r_{i2}'', s_{i2}', d_{12}, d_{22}, d_{32}, r_2, s_2)$, the receiver also computes

$$b_2 = [((s_{i2}')^2+1)/(s_{i2}^2+1)] \pmod q, \text{ and}$$

$$r_{i2}/(s_{i2}^2+1) = [(d_{12} r_{i2}')/((s_{i2}')^2+1)] \text{ mod } q.$$

If $r_i/(s_i^2+1) \equiv r_{i2}/(s_{i2}^2+1)$ (mod q), then $(m_2, r_{i2}', r_{i2}'', s_{i2}', d_{12}, d_{22}, d_{32}, r_2, s_2)$ is also generated by the user U_i. Therefore, Sun et al.'s scheme does not provide anonymity property.

On the other hand, anyone can determine whether or not $(m_1, r_{i1}', r_{i1}'', s_{i1}', d_{11}, d_{21}, d_{31}, r_1, s_1)$ and $(m_2, r_{i2}', r_{i2}'', s_{i2}', d_{12}, d_{22}, d_{32}, r_2, s_2)$ are generated by the same anonymous group member. Anyone is able to computes $r_{i1}/(s_{i1}^2+1)$ and $r_{i2}/(s_{i2}^2+1)$ for $(m_1, r_{i1}', r_{i1}'', s_{i1}', d_{11}, d_{21}, d_{31}, r_1, s_1)$ and $(m_2, r_{i2}', r_{i2}'', s_{i2}', d_{12}, d_{22}, d_{32}, r_2, s_2)$, respectively. If $r_i/(s_i^2+1) \equiv r_{i2}/(s_{i2}^2+1)$ (mod q), then $(m_1, r_{i1}', r_{i1}'', s_{i1}', d_{11}, d_{21}, d_{31}, r_1, s_1)$ and $(m_2, r_{i2}', r_{i2}'', s_{i2}', d_{12}, d_{22}, d_{32}, r_2, s_2)$ are generated by the same users. By the same way, all group signatures can be easily classified according to the anonymous signers. Therefore, Sun et al.'s scheme does not provide the unlinkability property.

4. CONCLUSIONS

In 2000, Sun et al. proposed a new group signature scheme. Sun et al. claimed that their scheme satisfies the seven properties in [3]. Moreover, Sun et al. also claimed that their scheme is also better than Lee and Chang scheme since Lee and Chang scheme does not provide unlinkability property. However, an attack is proposed to show that Sun et al.'s scheme does not provide anonymity and unlinkability properties.

REFERENCES

[1] Chaum, D., and F. Heyst, (1992): "Gropu signatures," Proc. EUROCRYPT'91, pp. 257-265, 1992.

[2] Lee, W.-B., and Chang, C.-C. (1998): "Efficient group signature scheme based on the discrete logarithm," IEE Proc. Comput. Digit. Tech., Vol. 145, No.1, pp. 15-18, 1998.

[3] Petersen, H. (1997): "How to convert any digital signature scheme into a group signature," Security Protocols Proceedings, Springer-Verlag, France, 1997, pp. 177-199.

[4] Sun, Ping-Tai, Chen, Jen-Rong, Chem, Jenn-Sheng, and Fang Gwo-Ching, (2000): "A New Scheme for the Lee and Chang Group Digital Signature," Proceedings of the Tenth National Conference on Information Security, Taiwan, 1999, pp. 126-130.