Forgery Attack on Improved Group Signature Scheme

Chien-Lung Hsu (許建隆)
Department of Information Management
National Taiwan University of Science and Technology
Taipei, Taiwan 106, Republic of China
E-mail: clhsu_journal@yahoo.com.tw

Tzong-Sun Wu (吳宗杉)
Department of Informatics
Fo Guang University
I-Lan, Taiwan 262, Republic of China
E-mail: tswu@mail.fgu.edu.tw

Ming-Jheng Li (李明政)
Department of Informatics
Fo Guang University
I-Lan, Taiwan 262, Republic of China
E-mail: g1332014@stdmail.fgu.edu.tw

Ming-Je Shiu (許明哲)
Department of Informatics
Fo Guang University
I-Lan, Taiwan 262, Republic of China
E-mail: a4325830@ms23.hinet.net

Abstract

The authors demonstrate that Tseng and Jan's improved group signature scheme based on the discrete logarithm problem cannot satisfies the *revocability* and *unforgeability* properties under the attacks of the insider forgery and the universal forgery attacks.

***Key words*:** group signature, insider forgery attack, universal forgery attack

1. Introduction

In 1991, Chaum and van Heyst [1] introduced the concept of group signature scheme which allows any group member to sign messages on behalf of the group. Any verifier can validate the group signature with a single group public key, while he cannot discover the identity of the signer. In case of a later dispute, a group authority or the group members together can open the signature to reveal the identity of the signer to the verifier.

In 1998, Lee and Chang proposed an efficient group signature scheme based on the discrete logarithm problem [2]. However, Tseng and Jan [5] pointed out that the Lee-Chang scheme does not provide the *unlinkability* property [3], i.e., the group signatures generated by the same group member can be identified by the verifier. They further proposed an improvement to resolve this problem [5]. Unfortunately, Sun [4] gave a comment on Tseng and Jan's improvement that the scheme is still not unlinkable. After that, Tseng and Jan [6] tried to propose another improvement to eliminate this drawback. In this letter, however, we will show that the new Tseng-Jan improvement [6] still cannot satisfies the *revocability* and the *unforgeability* properties which refer to that the identity of the signer can be identified by "opening" the group signature in case of a later dispute and the group signature is not forgeable by any unauthorized person(s), respectively [3].

2. Review of the Tseng-Jan improvement

The Tseng-Jan improvement consists of three phases: the initialization, the signature generation and verification, and the identification phases. The first and second phases are stated in the following, while the last one is omitted since it is irrelevant to the discussion of this letter. Detailed description of the identification phase can be referred to [6].

(1) *Initialization phase*: Let T be the authority of the group and whose responsibilities are performing the initial setup and identifying the signer in case of a later dispute. Let p be a large prime, q a large prime factor of $p - 1$, g a generator with order q in GF(p), and h a one-way hash function. T owns a private key $x_T \in Z_q^*$ and a public key $y_T = g^{x_T} \bmod p$. Similarly, each group member U_i owns his private and public keys as $x_i \in Z_q^*$ and $y_i = g^{x_i} \bmod p$, respectively. For each group

member U_i, T chooses an integer $k_i \in Z_q^*$ and computes $r_i = g^{-k_i} \cdot DH_i \bmod p$ and $s_i = k_i - r_i \cdot x_T \bmod q$, where $DH_i = y_i^{k_i} \bmod p$. Then, T stores (r_i, s_i, k_i), which will be needed for identifying the signer in case of a later dispute, and sends (r_i, s_i) to U_i secretly. Upon receiving (r_i, s_i), U_i can verify its validity by checking that

$$g^{s_i} \cdot y_T^{r_i} \cdot r_i = (g^{s_i} \cdot y_T^{r_i})^{x_i} \pmod p \qquad (1)$$

If it holds, U_i keeps (r_i, s_i) secret and which can be used to generate group signatures.

(2) *Signature generation and verification phase*: For signing the message m on behalf of the group, the group member U_i chooses four random integers a, b, d, t in Z_q^* and computes

$$A = r_i^{a} \bmod p$$

$$B = a \cdot s_i - b \cdot h(A, C, D, E) \bmod q$$

$$C = r_i \cdot a - d \bmod q$$

$$D = g^{b} \bmod p$$

$$E = y_T^{d} \bmod p$$

$$\alpha_i = g^{B} \cdot y_T^{C} \cdot E \cdot D^{h(A,C,D,E)} = g^{a \cdot k_i} \pmod p$$

$$R = \alpha_i^{t} = g^{a \cdot k_i \cdot t} \pmod p$$

Then, U_i derives S from the congruence relation $h(m, R) = t \cdot S + R \cdot x_i \bmod q$. The group signature for m is (R, S, A, B, C, D, E). Upon receiving the signature, the verifier first computes α_i and DH_i as

$$\alpha_i = g^{B} \cdot y_T^{C} \cdot E \cdot D^{h(A,C,D,E)} \bmod p \qquad (2)$$

$$DH_i = \alpha_i \cdot A \bmod p \qquad (3)$$

and then validates the group signature by checking that

$$\alpha_i^{h(m,R)} = DH_i^{R} \cdot R^{S} \pmod p \qquad (4)$$

If it holds, the verifier accepts the signature as a valid one.

3. Attacks on the Tseng-Jan improvement

Here we demonstrate two attacks on the Tseng-Jan scheme: the insider forgery and the universal forgery attacks. The insider forgery attack refers to that some malicious registered group member U_i can use his private key x_i and (r_i, s_i) to produce a new (r_i', s_i', x_i'), and then use (r_i', s_i', x_i') to generate a group signature such that U_i will not be identified when the signature is "opened" by *T*. The universal forgery attack refers to that any adversary can generate a valid group signature without knowing any secret information. It can be seen that the *revocability* and the *unforgeability* properties are violated under the first and the second attacks, respectively.

(1) *Insider forgery attack*: For performing this attack, any registered group member, say U_i with the knowledge of (r_i, s_i, x_i), first chooses an integer $u \in Z_q$ and computes $r_i' = g^{u} r_i \bmod p$. Then, U_i finds (s_i', x_i') satisfying both the congruence relations: $r_i' \cdot (x_i' - 1) = r_i \cdot (x_i - 1) \pmod q$ and $s_i' \cdot (x_i' - 1) = s_i \cdot (x_i - 1) + u \pmod q$. Note that (s_i', x_i') can be uniquely determined since there are two unknown variables in two congruence relations. Thereafter, U_i can use (r_i', s_i', x_i') to generate valid group signatures, which is not revocable, i.e. U_i will not be identified. Here, we show that (r_i', s_i', x_i') can be used to generate valid signatures. That is, (r_i', s_i', x_i') satisfies the equality of Eq. (1).

$$g^{s_i} \cdot y_T^{r_i} \cdot r_i = (g^{s_i} \cdot y_T^{r_i})^{x_i} \pmod p$$

$$\Leftrightarrow r_i = (g^{s_i} \cdot y_T^{r_i})^{(x_i - 1)} \pmod p$$

$$\Leftrightarrow g^{u} \cdot r_i = g^{s_i \cdot (x_i - 1) + u} \cdot y_T^{r_i \cdot (x_i - 1)} \pmod p$$

$$\Leftrightarrow r_i' = g^{s_i' \cdot (x_i' - 1)} \cdot y_T^{r_i' \cdot (x_i' - 1)} \pmod p$$

$$\Leftrightarrow g^{s_i'} \cdot y_T^{r_i'} \cdot r_i' = (g^{s_i'} \cdot y_T^{r_i'})^{x_i'} \pmod p$$

(2) *Universal forgery attack*: Consider the scenario that the adversary attempts to forge a valid group signature $(R', S', A', B', C', D', E')$ for the chosen message m' without the knowledge of any secret information. The adversary first chooses six integers $s, r, k, a, b, d \in Z_q^*$, and then computes

$$A' = \left(g^{a \cdot s} \cdot y_T^{a \cdot r}\right)^k \bmod p$$

$$C' = a \cdot r - d \bmod q$$

$$D' = g^b \bmod p$$

$$E' = y_T{}^d \bmod p$$

$$B' = a \cdot s - b \cdot h(A', C', D', E') \bmod q$$

$$R' = (g^{a \cdot s} \cdot y_T{}^{a \cdot r})^t \bmod p \qquad (5)$$

$$S' = t^{-1} \cdot (h(m', R') - (k+1) \cdot R') \bmod q \qquad (6)$$

Here, we show that $(R', S', A', B', C', D', E')$ can be served as a valid group signature, i.e. it can pass the group signature verification of Eq. (4). From Eqs. (2) and (3), we have

$$\alpha_i' = g^{B'} \cdot y_T{}^{C'} \cdot E' \cdot D'^{h(A',C',D',E')}$$
$$= (g^{a \cdot s} \cdot y_T^{a \cdot r})(\text{mod } p) \qquad (7)$$

$$DH_i = \alpha_i' \cdot A' = (g^{a \cdot s} \cdot y_T{}^{a \cdot r})^{(k+1)} (\text{mod } p) \qquad (8)$$

Thus,

$$R'^{S'} \cdot DH_i{}^{R'}$$
$$= (g^{a \cdot s} \cdot y_T{}^{a \cdot r})^{tS'} \cdot (g^{a \cdot s} \cdot y_T{}^{a \cdot r})^{(k+1)R'}$$
(by Eqs. (5) and (8))

$$= \alpha_i^{tS' + (k+1)R'}$$ (by Eq. (7))

$$= \alpha_i^{h(m',R')} (\text{mod } p)$$ (by Eq. (6))

4. Conclusions

We have demonstrated that the Tseng and Jan's improved group signature scheme [6] cannot withstand the insider forgery and the universal forgery attacks and thus their scheme is failed to achieve the properties of *revocability* and *unforgeability*.

5. References

[1] D. Chaum and E. van Heyst, "Group signature, *Advances in Cryptology - EUROCRYPT'91*," pp. 257-265, Springer-Verlag, Brighton, 1991.

[2] W.B. Lee and C.C. Chang, "Efficient group signature scheme based on the discrete logarithm," *IEE Proceedings Computers and Digital Techniques*, vol. 145, no. 1, pp. 15-18, 1998.

[3] H. Petersen, "How to convert any digital signature scheme into a group signature scheme," *Security Protocols Proceedings*, pp. 177-190, Springer-Verlag, France, 1997.

[4] H.M. Sun, "Comment: Improved group signature scheme based on discrete logarithm problem," *Electronics Letters*, vol. 35, no. 16, pp. 1323-1324, 1999.

[5] Y.M. Tseng and J.K. Jan, "Improved group signature scheme based discrete logarithm problem," *Electronics Letters*, vol. 35, no. 1, pp. 37-38, 1999.

[6] Y.M. Tseng and J.K. Jan, "Reply: Improved group signature scheme based discrete logarithm problem," *Electronics Letters*, vol. 35, no. 16, pp. 1324-1325, 1999.