A New Group Signature Scheme Based on the Discrete Logarithm

Cheng-Chi Lee[1] , Ting-Yi Chang[2] and Min-Shiang Hwang[3,4]

[1]Department of Photonics and Communication Engineering
Asia University
No. 500, Lioufeng Road,
Wufeng Shiang, Taichung, Taiwan 413, R.O.C.
cclee@asia.edu.tw
[2]Department of Business Education,
Graduate Institute of e-Learing,
National Changhua University of Education
No. 1, Jin-De Road, Changhua City, Taiwan, R.O.C.
tychang@cc.ncue.edu.tw
[3]Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
mshwang@nchu.edu.tw
[4]corresponding author

Abstract: In 1998, Lee and Chang proposed an efficient group signature scheme based on the discrete logarithm. In the Lee-Chang scheme, when the signer has been identified, the authority has to redistribute the keys of this signer and send the keys to him/her. Otherwise, all the previous group signatures are linkable at the same time and any verifier will identify all future group signatures not through the authority. It is not feasible for the applications of the group signatures. In this paper, the authors shall propose an improvement of the Lee-Chang scheme to solve the above problems.

Keywords: Group signature, unforgeable, unlinkable, security.

1 Introduction

In 1991, Chaum and Heyst proposed a new type of signature called group signature [2, 3, 11], which is defined in [1] to allow individual member to make a signature on behalf of the group' which has the following three properties:

- Only the legitimate members of the group can sign a message.
- Any receiver is able to verify that signature as a valid group signature, but he/she has no ability to detect which group member signed the message.
- In the case of a dispute, the signature must be opened only by the group authority or all the group members' cooperation.

However, four signature schemes were presented in Chaum-Heyst's paper, when the group is changed, it must affect all distributed secret keys. And the four signature schemes belong to the interactive system, which is very inefficient.

In 1997, Park, Kim and Won [10] proposed an ID-based group signature. The main contribution of their scheme is that signer's public key is an identification (ID) that does not need to be verified, so there is no need to set up a trusted center to verify a huge number of public keys. Nevertheless, an ID-based group signature must use a set of group member identities in the signing phase. When the group changes, the group signature is inactive. Moreover, the length of its signature increases with the number of members.

In 1998, Lee and Chang [5] proposed an efficient group signature based on the discrete logarithm [4, 13, 14]. The scheme was more efficient in terms of computational, communication and storage costs, while allowing the group to be changed without having the members choosing the new keys. However, when the signer has been identified, the authority must redistribute the keys of this signer and send the keys to him/her.

In 1999, Tseng and Jan [15] aimed to improve the aforementioned problem to propose an improved group signature that is based on the Lee-Chang scheme. In the same year, Sun showed in [12] that the Tseng-Jan scheme is still not unlinkable. After that, Tseng-Jan [16] proposed to improve their scheme. In 2000, Li [6] et al. demonstrated that two schemes of the Tseng-Sun's paper, which are called TJ1 and TJ2 in Li et al's paper, both could be attacked.

In this article, we shall propose an improvement on the Lee-Chang scheme based on the discrete logarithm. In our scheme, when the signer has been identified, the group authority needs not to redistribute any of the keys of this signer. Our scheme is not only it is unlinkable, but also Li et al. cannot forge an attack.

The remainder of this paper is organized as follows. In Section 2, we briefly review the Lee-Chang scheme. In Section 3, we propose an improvement on the Lee-Chang scheme. In Section 4, we analyze the security of our scheme. Finally, we give a brief conclusion.

2 Review of the Lee-Chang Scheme

The Lee-Chang scheme is composed of three phases: (1) *the initiation phase*, (2) *the signing and verification phase*, and (3) *the identification phase*. We briefly describe the three phases as follows:

1. Initiation phase: Let p and q be two large primes such that

$q|p-1$. Let g be a generator with order q in $GF(p)$. Every group member U_i chooses the secret key x_i and computes the public key $y_i = g^{x_i} \bmod p$. Let T be the group authority which has the secret key x_T and the public key $y_T = g^{x_T} \bmod p$. T chooses a random number k_i, where $\gcd(k_i, q) = 1$ and computes $r_i = g^{-k_i} y_i^{k_i} \bmod p$ and $s_i = k_i - r_i x_T \bmod q$ for each group member. Then T sends (r_i, s_i) to the group member U_i secretly. After receiving (r_i, s_i), U_i can verify the information by checking congruence relation $g^{s_i} y_T^{r_i} r_i = (g^{s_i} y_T^{r_i})^{x_i} \bmod p$.

2. Signing and verification phase: To sign message m, U_i chooses a random number $t \in Z_p^*$. Then U_i computes $r = \alpha_i^t \bmod p$, where $\alpha_i = g^{s_i} y_T^{r_i} \bmod p = g^{k_i} \bmod p$, and solves the congruence relation $h(m) = rx_i + ts \bmod q$ for the parameter s, where $h(\cdot)$ denotes a one-way hash function. The group signature is $\{h(m), r, s, (r_i, s_i)\}$, After receiving the information $\{h(m), r, s, (r_i, s_i)\}$, any receiver can verify the group signature through the following steps:
   (a) Compute $\alpha_i = g^{s_i} y_T^{r_i} \bmod p$.
   (b) Compute $DH_i = \alpha_i r_i \bmod p$.
   (c) Check the congruence relation $\alpha_i^{h(m)} = r^s DH_i^r \bmod p$.

   If the above relation holds, the group signature is valid.

3. Identification phase: In the case of a dispute, the group authority has the ability to identify the signature that a group member has signed and announce some information to convince the verifier that U_i is indeed the signer. Because the authority has the knowledge of the secret key x_T, k_i can be solved from the equation as:

$$k_i = s_i + r_i x_T \bmod q.$$

   The authority can further obtain y_i from DH_i as:

$$DH_i = y_i^{k_i} \bmod p.$$

Hence, when the signer is identified, the linkage between (r_i, s_i) and y_i is constructed. If U_i wants to sign another message m', the group signature for m' is $\{r', s', h(m'), (r_i, s_i)\}$. The pair keys (r_i, s_i) of the group signature $\{r', s', h(m'), (r_i, s_i)\}$ are not change, so any verifier can identify the signer that is the same signer U_i. In other words, it is not unlinkable [15]. According to the above statement to be improved, the authority must redistribute the pair keys (r_i, s_i) and send to U_i.

3 Our Scheme

In this section, we propose an improvement of the Lee-Chang scheme. The improvement also consists of three phases: (1) *the initiation phase*, (2) *the signing and verification phase*, and (3) *the identification phase*. The initiation phase is the same as that of the Lee-Chang scheme. Besides, the authority keeps each group member's k_i. We describe the other phases in detail as follows:

Signing and verification phase:
Suppose U_i wants to sign the message m by the following steps.

1. Randomly choose two random numbers w and z such that the greatest common divisor of w and z, denoted by $gcd(w, z)$, is 1. When $gcd(w, z) = 1$, there must be exactly two integers e and d that satisfy the equation $ew + dz = 1$. It is called the Extended Euclidean algorithm [7].
2. Randomly choose a random number a and a constant c.
3. Compute $\{R_1, R_2, S_1, S_2, A, B\}$ as

$$\begin{aligned} R_1 &= a \cdot c \cdot e \cdot w \cdot r_i \bmod p, \\ R_2 &= a \cdot c \cdot d \cdot z \cdot r_i \bmod p, \\ S_1 &= a \cdot c \cdot e \cdot w \cdot s_i \bmod q, \\ S_2 &= a \cdot c \cdot d \cdot z \cdot s_i \bmod q, \\ A &= r_i^{ac} \bmod p, \\ B &= y_T^{x_i} ac \bmod p. \end{aligned}$$

4. Compute $\alpha_1, \alpha_2, \alpha_i$ as

$$\begin{aligned} \alpha_1 &= g^{S_1} y_T^{R_1} \bmod p, \\ \alpha_2 &= g^{S_2} y_T^{R_2} \bmod p, \\ \alpha_i &= \alpha_1 \cdot \alpha_2 \bmod p. \end{aligned}$$

5. Randomly choose a number $t \in Z_p^*$ and compute $R = \alpha_i^t \bmod p$. Then solves the congruence relation $h(m) = Rx_i + tS \bmod q$ for the parameter S. The information $\{h(m), R, S, R_1, R_2, S_1, S_2, A, B\}$ is the group signature.

After receiving the information $\{h(m), R, S, R_1, R_2, S_1, S_2, A, B\}$, any verifier can validate the group signature by the following steps.

1. Compute $\alpha_1, \alpha_2, \alpha_i$ as

$$\begin{aligned} \alpha_1 &= g^{S_1} y_T^{R_1} \bmod p, \\ \alpha_2 &= g^{S_2} y_T^{R_2} \bmod p, \\ \alpha_i &= \alpha_1 \cdot \alpha_2 \bmod p. \end{aligned}$$

2. Compute $DH_i = \alpha_i A \bmod p$.
3. Verify the congruence relation as follows.

$$\alpha_i^{h(m)} = R^S DH_i^R \bmod p. \qquad (1)$$

If the above relation holds, then the group signature is valid. In order to prove the correctness of Equation (1), we first show the computation of $\alpha_1, \alpha_2, \alpha_i$, and DH_i as follows.

$$\begin{aligned} \alpha_1 &= g^{S_1} y_T^{R_1} \\ &= g^{S_1} g^{x_T R_1} \\ &= g^{a \cdot c \cdot e \cdot w \cdot s_i} g^{x_T \cdot a \cdot c \cdot e \cdot w \cdot r_i} \\ &= g^{a \cdot c \cdot e \cdot w \cdot (k_i - r_i x_T)} g^{x_T \cdot a \cdot c \cdot e \cdot w \cdot r_i} \\ &= g^{a \cdot c \cdot e \cdot w \cdot k_i} \bmod p, \end{aligned}$$

$$\begin{aligned} \alpha_2 &= g^{S_2} y_T^{R_2} \\ &= g^{S_2} g^{x_T R_2} \\ &= g^{a \cdot c \cdot d \cdot z \cdot s_i} g^{x_T \cdot a \cdot c \cdot d \cdot z \cdot r_i} \\ &= g^{a \cdot c \cdot d \cdot z \cdot (k_i - r_i x_T)} g^{x_T \cdot a \cdot c \cdot d \cdot z \cdot r_i} \\ &= g^{a \cdot c \cdot d \cdot z \cdot k_i} \bmod p, \end{aligned}$$

$$\begin{aligned} \alpha_i &= \alpha_1 \cdot \alpha_2 \\ &= g^{a \cdot c \cdot e \cdot w \cdot k_i} g^{a \cdot c \cdot d \cdot z \cdot k_i} \\ &= g^{a \cdot c \cdot k_i \cdot (ew + dz)} \\ &= g^{a \cdot c \cdot k_i} \bmod p, \end{aligned}$$

$$\begin{aligned} DH_i &= \alpha_i A \\ &= \alpha_i r_i^{ac} \\ &= g^{a \cdot c \cdot k_i} (g^{-k_i} y_i^{k_i})^{ac} \\ &= g^{a \cdot c \cdot k_i} (g^{-k_i} g^{x_i k_i})^{ac} \\ &= g^{a \cdot c \cdot k_i} g^{-a \cdot c \cdot k_i} g^{x_i \cdot k_i \cdot a \cdot c} \\ &= g^{x_i \cdot k_i \cdot a \cdot c} \bmod p. \end{aligned}$$

The correctness of Equation (1) can be verified as follows.

$$\begin{aligned} \alpha_i^{h(m)} &= \alpha_i^{Rx_i + tS}, \\ &= R^S \alpha_i^{Rx_i}, \\ &= R^S (g^{ack_i})^{Rxi}, \\ &= R^S DH_i^R \bmod p. \end{aligned}$$

Identification phase:
In the case of dispute, the group signature must be opened to reveal the identity of the signer. Here we show how to open the group signature $\{h(m)$, R, S, R_1, R_2, S_1, S_2, A, B$\}$ by the following steps.

1. The authority first chooses a candidate y_i and computes

$$(ac)' = By_i^{-x_T} \bmod p.$$

2. Since the authority has access to the key k_i of each group member U_i, he/she can compute r_i as

$$r_i = g^{-ki} y_i^{k_i} \bmod p.$$

3. Compute $(R_1 + R_2)/r_i$ to acquire $a \cdot c$.

$$\begin{aligned}(R_1 + R_2)/r_i &= [(a \cdot c \cdot e \cdot w \cdot r_i) + (a \cdot c \cdot d \cdot z \cdot r_i)]/r_i,\\ &= [a \cdot c \cdot r_i(ew + dz)]/r_i,\\ &= a \cdot c \bmod p.\end{aligned}$$

4. Once the authority acquire ac, the ac is compared with the $(ac)'$. If the two acs are equal, we can ensure that the y_i is U_i's public key. Otherwise, try the next candidate y_i.
5. Randomly choose a number b.
6. Compute $r_T = (gy_i)^{acb} \bmod p$.
7. Compute $s_T = acb - acr_T k_i \bmod q$.
8. Send (r_T, s_T) to verifier and announce that user U_i is the signer.

On receiving the announcement from the authority, the verifier needs to check the correctness of the announcement as following steps.

1. Compute $\beta_i = gy_i \bmod p$, where y_i is the signer U_i's public key.
2. Compute $\delta_i = \alpha_i DH_i \bmod q$.
3. Verify the congruence relation

$$r_T = \beta_i^{s_T} \delta_i^{r_T} \bmod p. \quad (2)$$

The correctness of Equation (2) can be verified as follows:

$$\begin{aligned}r_T &= (gy_i)^{acb},\\ &= g^{acb+acbx_i} \bmod p;\end{aligned}$$

and

$$\begin{aligned}\beta_i^{s_T} \delta_i^{r_T} &= (gy_i)^{s_T} (\alpha_i DH_i)^{r_T},\\ &= (gy_i)^{s_T} (g^{ac(k_i + x_i k_i)})^{r_T},\\ &= g^{x_i s_T} g^{s_T} g^{ac(k_i + x_i k_i) r_T},\\ &= g^{x_i(acb - acr_T k_i)} g^{acb - acr_T k_i} g^{ack_i r_T + acr_T x_i k_i},\\ &= g^{acbx_i - acr_T k_i x_i} g^{acb - acr_T k_i} g^{ack_i r_T + acr_T x_i k_i},\\ &= g^{acb+acbx_i} \bmod p.\end{aligned}$$

According to the above steps, the identity U_i with y_i can be identified by the authority and the verifier.

4 Security Analysis

In this section, we analyze the security of our scheme. Our scheme is unlinkable and unforgeable.

Unlinkable:

After identifying the group signature for m is $\{h(m), R, S, R_1, R_2, S_1, S_2, A, B\}$, the verifier knows who make this signature from the authority's announcement. If U_i wants to sign another message m', the group signature for m' is $\{h(m'), R', S', R_1', R_2', S_1', S_2', A', B'\}$. There are no the same parameters in $\{h(m), R, S, R_1, R_2, S_1, S_2, A, B\}$ and $\{h(m'), R', S', R_1', R_2', S_1', S_2', A', B'\}$. So when verifier wants to know the group signature $\{h(m'), R', S', R_1', R_2', S_1', S_2', A', B'\}$ who make the signature must through the authority. Moreover, our scheme has four parameters (e, w, d, z) to hide the true value of r_i and s_i. It is hard to reveal r_i and s_i from the group signature. Besides, if the verifier wants to find the linkability between $\{h(m), R, S, R_1, R_2, S_1, S_2, A, B\}$ and $\{h(m'), R', S', R_1', R_2', S_1', S_2', A', B'\}$. It is the same as hard as to reveal r_i and s_i.

Unforgeable:

Li [6] et al. demonstrated that two schemes of the Tseng-Sun's papers, which are called TJ1 and TJ2 in Li et al's paper, both could be forgery attacked. TJ1 and TJ2 can be found the special equations to forgery (Refer to [6] for more details.). As we all know, Li et al. cannot forgery attack on the Lee-Chang scheme.

Our scheme adds two parameters: a and c in the exponent operation of the verification phase to enhance the security. Besides, the security of our scheme is based on the discrete logarithm [8, 9], which is the same as that of Lee-Chung's scheme. Therefore, it is difficult to forgery attack on our scheme.

5 Conclusions

In this article, we have proposed an improved group signature scheme based on the Lee-Chang scheme. In our scheme, when the singer has been identified, the group authority needs not to redistribute any of the keys of this signer. Furthermore, our scheme is unlinkable and cannot be attacked by forgers.

Acknowledgments

This work was supported in part by the Taiwan Information Security Center (TWISC) and the National Science Council under the grants NSC96-2219-E-009-013 and NSC98-2221-E-468-002.

References

[1] D. Chaum and E. Heyst, "Group signatures," in *Advances in Cryptology, Eurocrypt'91*, pp. 257–265, Lecture Notes in Computer Science, 1991.

[2] He Ge, "An Effective Method to Implement Group Signature with Revocation," *International Journal of Network Security*, vol. 5, no. 2, pp. 134–139, 2007.

[3] Maged Hamada Ibrahim, "Resisting Traitors in Linkable Democratic Group Signatures," *International Journal of Network Security*, vol. 9, no. 1, pp. 51–60, 2009.

[4] C. C. Lee, W. H. Ku, and S. Y. Huang, "On the Security of Sehkar's Signature Schemes," *Journal of Information Assurance and Security*, vol. 2, no. 2, pp. 75–76, 2007.

[5] W.B. Lee and C.C. Chang, "Efficient group signature scheme based on the discrete logarithm," *IEE Proc.-Computer Digital Technology*, vol. 145, no. 1, pp. 15–18, 1998.

[6] Zichen Li, L.C.K. Hui, K.P. Chow, C.F. Chong, W.W. Tsang, and H.W. Chan, "Security of Tseng-Jan's group signature schemes," *Information Processing Letters*, vol. 75, no. 5, pp. 187–189, 2000.

[7] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography.* CRC Press, 1996.

[8] Min-Shiang Hwang and Ting-Yi Chang, "Threshold Signatures: Current Status and Key Issues," *International Journal of Network Security*, vol. 1, no. 3, pp. 123–137, 2005.

[9] Min-Shiang Hwang and Cheng-Chi Lee, "Research Issues and Challenges for Multiple Digital Signatures," *International Journal of Network Security*, vol. 1, no. 1, pp. 1–7, 2005.

[10] S. Park, S. Kim, and D. Won, "ID-based group signature," *IEE Electronics Letters*, vol. 33, no. 19, pp. 1616–1617, 1997.

[11] Zuhua Shao, "Repairing Efficient Threshold Group Signature Scheme," *International Journal of Network Security*, vol. 7, no. 2, pp. 218–222, 2008.

[12] Hung-Min Sun, "Comment improved group signature scheme based on discrete logarithm problem," *IEE Electronics Letters*, vol. 35, no. 16, pp. 1323–1324, 1999.

[13] N. R. Sunitha and B. B. Amberker, "Proxy Signature Schemes for Controlled Delegation," *Journal of Information Assurance and Security*, vol. 3, no. 2, pp. 159–174, 2009.

[14] N. R. Sunitha and B. B. Amberker, "Some Aggregate Forward-Secure Signature Schemes," *Journal of Information Assurance and Security*, vol. 4, no. 1, pp. 84–90, 2009.

[15] Yuh-Min Tseng and Jinn-Ke Jan, "Improved group signature scheme based on discrete logarithm problem," *IEE Electronics Letters*, vol. 35, no. 1, pp. 37–38, 1999.

[16] Yuh-Min Tseng and Jinn-Ke Jan, "Reply improved group signature scheme based on discrete logarithm problem," *IEE Electronics Letters*, vol. 35, p. 1324, 1999.