On the Security of the Lee-Chang Group Signature Scheme and its Derivatives
(Extended Abstract)*

[Published in M. Mambo and Y. Zheng, Eds., *Information Security*, vol. 1729 of *Lecture Notes in Computer Science*, pp. 47–51, Springer-Verlag, 1999.]

Marc Joye[1,**], Narn-Yih Lee[2], and Tzonelih Hwang[3]

[1] Gemplus Card International
Parc d'Activités de Gémenos, B.P. 100, 13881 Gémenos, France
marc.joye@gemplus.com
[2] Dept of Applied Foreign Language, Nan-Tai Institute of Technology
Tainan, Taiwan 710, R.O.C.
nylee@mail.ntc.edu.tw
[3] Institute of Information Engineering, National Cheng-Kung University
Tainan, Taiwan, R.O.C.
hwangtl@server2.iie.ncku.edu.tw

Abstract. W.-B. Lee and C.-C. Chang (1998) proposed a very efficient group signature scheme based on the discrete logarithm problem. This scheme was subsequently improved by Y.-M. Tseng and J.-K. Jan (1999) so that the resulting group signatures are unlinkable. In this paper, we show that any obvious attempt to make unlinkable the Lee-Chang signatures would likely fail. More importantly, we show that both the original Lee-Chang signature scheme and its improved version are universally forgeable.

Keywords. Digital signatures, group signatures, cryptanalysis.

1 Group Signatures

A *group signature* [1] is a digital signature that allows a group member to sign a message on behalf of the group so that (i) only group members are able to sign on behalf of the group, (ii) it is not possible to determine which group member made the signature, and (iii) in case of disputes, the group authority can "open" the signature to reveal the identity of the signer.

* The full paper is available as technical report (LCIS TR-99-7, May 1999) at http://www.ee.tku.edu.tw/~lcis/techreports/1999/TR-99-7.html.

** Part of this work was performed while the author was with the Dept of Electrical Engineering, Tamkang University, Tamsui, Taiwan 251, R.O.C.

Group signatures can be used to conceal organizational structures, e.g., when a company or a government agency issues a signed statement. They can also be integrated into an electronic cash system in which several banks can securely distribute anonymous and untraceable e-cash. The group property presents then the further advantage to also conceal the identity of the issuing bank [3].

2 Lee-Chang Group Signature

We first begin with a brief review of the Lee-Chang group signature scheme and refer to [2] for a thorough description.

For setting up the system, the group authority, T, selects two large primes p and q so that q divides $(p-1)$. He also chooses a generator g of the (multiplicative) subgroup of order q of $\mathrm{GF}(p)$. Finally, he chooses a secret key x_T and computes $y_T = g^{x_T} \bmod p$. The group authority makes public p, q, g and y_T. When a user, say U_i, wants to join the group, he first chooses a secret key x_i and computes his corresponding public key $y_i = g^{x_i} \bmod p$. From this public key, the group authority then computes $r_i = g^{-k_i}\, {y_i}^{k_i} \bmod p$ and $s_i = k_i - r_i\, x_T \bmod q$ for a randomly chosen k_i. The membership certificate of user U_i is the pair (r_i, s_i).

Given a membership certificate, any group member is now able to sign a message on behalf of the group. Let m be the message that user U_i wants to sign on behalf of the group and let $h(\cdot)$ be a publicly known one-way hash function. User i first computes $\alpha_i = {y_T}^{r_i}\, g^{s_i} \bmod p$. Next, he chooses a random number t, computes $r = {\alpha_i}^t \bmod p$, and solves for s the congruence $h(m) \equiv r x_i + t s \pmod q$. The group signature on message m is given by (r, s, r_i, s_i).

Anyone can now check the validity of this signature by first computing $\alpha_i = {y_T}^{r_i}\, g^{s_i} \bmod p$ and $DH_i = \alpha_i\, r_i \bmod p$, and then checking whether

$$ {\alpha_i}^{h(m)} \equiv r^s\, {DH_i}^r \pmod p \tag{1} $$

holds or not. Moreover, the group authority knows that this signature was issued by user U_i since he knows that the pair (r_i, s_i) corresponds to that user.

3 Unlinkability

The main property of group signatures is that they allow group members to *anonymously* sign on behalf of the group. A related desirable property is that of *unlinkability*. Two different group signatures are unlinkable if no one (but the group authority) is able to decide whether these signatures were issued by the same group member. In the Lee-Chang scheme, the signatures are obviously linkable since each signature generated by user U_i contains the pair (r_i, s_i). The utility of the Lee-Chang scheme appears thus to be somewhat limited in the context of group signatures, as defined in [1].

4 Tseng-Jan Improved Group Signature

Making the Lee-Chang group signature scheme unlinkable seems easy: it suffices not to send (r_i, s_i) and to modify the signature accordingly. This was first proposed and realized by Tseng and Jan [5].

In their scheme, the system setup is the same as in the Lee-Chang scheme (see Section 2). To sign a message m, user U_i with membership certificate (r_i, s_i) randomly chooses a, b and computes the five quantities $A = {r_i}^a \bmod p$, $B = s_i - b \bmod q$, $C = r_i\, a \bmod q$, $D = g^a \bmod p$ and $E = g^{ab} \bmod p$. He then computes $\alpha_i = D^B\, {y_T}^C\, E \bmod p$ and $r = {\alpha_i}^t \bmod p$ for a randomly chosen t. He finally solves for s the congruence $h(m) \equiv r x_i + t s \pmod q$. The group signature on message m is (r, s, A, B, C, D, E). This signature can be validated by verifying that

$$ {\alpha_i}^{h(m)} \equiv {DH_i}^r\, r^s \pmod p \tag{2} $$

with $\alpha_i = D^B\, {y_T}^C\, E \bmod p$ and $DH_i = \alpha_i\, A \bmod p$. Finally, in case of disputes, the group authority can recover which member issued a given signature by checking for which value of k_i (and thus for which user U_i, see Section 2) the congruence $D^{k_i} \equiv D^B\, {y_T}^C\, E \pmod p$ is satisfied.

5 Cryptanalysis

As already remarked by Lee and Chang [2, Section 2], it is worth observing that the membership certificate (r_i, s_i) of user U_i is a Nyberg-Rueppel signature [4] on "message" DH_i ($\equiv {y_i}^{k_i} \equiv {y_T}^{r_i}\, g^{s_i}\, r_i \pmod p$). We analyze the implications in the next two paragraphs. Next, in § 5.3, we will show how to universally forge a valid group signature without membership certificate.

5.1 Lee-Chang signature

Let us first explain how given the membership certificate (r_i, s_i),[1] an adversary can create a new membership certificate (r'_i, s'_i) in the Lee-Chang scheme for a chosen "message" μ. The adversary first recovers DH_i as $DH_i = \alpha_i\, r_i \bmod p$ where $\alpha_i = {y_T}^{r_i}\, g^{s_i} \bmod p$. Next, for a chosen "message" μ, he applies Chinese remaindering to $r'_{i,p} = {\alpha_i}^{-1}\, \mu \bmod p$ and $r'_{i,q} = r_i \bmod q$ to obtain r'_i as

$$ r'_i = r'_{i,p} + p\,[p^{-1}(r'_{i,q} - r'_{i,p}) \bmod q] \ . \tag{3} $$

(Note that $r'_i > p$.) He also sets $s'_i = s_i$. One can easily see that, *provided that the range conditions are not checked*, (r'_i, s'_i) will be accepted as a valid Nyberg-Rueppel signature on message μ. Indeed, since $r'_i \equiv r_i \pmod q$ and $s'_i = s_i$, it follows that $\alpha'_i :\equiv {y_T}^{r'_i}\, g^{s'_i} \equiv {y_T}^{r_i}\, g^{s_i} \equiv \alpha_i \pmod p$, and therefore, noting that $r'_i \equiv {\alpha_i}^{-1}\, \mu \pmod p$, (r'_i, s'_i) is the Nyberg-Rueppel signature on $DH'_i :\equiv \alpha'_i\, r'_i \equiv \alpha_i\, {\alpha_i}^{-1}\, \mu \equiv \mu \pmod p$. If we now take a closer look at the verification equation in the Lee-Chang signature (i.e., Eq. (1)), we see that if μ is chosen as a power of α_i, i.e., $\mu = {\alpha_i}^w \bmod p$ for a randomly chosen w, then

[1] We note that (r_i, s_i) is publicly available from any given group signature.

solving for s the congruence $h(m) \equiv st + wr \pmod{q}$ —where as in the original scheme $r = {\alpha_i}^t \bmod p$ for a randomly chosen t— yields a valid group signature (r, s, r'_i, s'_i).

5.2 Tseng-Jan signature

We now return to the Tseng-Jan group signature scheme. This scheme may be seen as the Lee-Chang scheme where user U_i sends a "randomized" membership certificate (A, B, C, D, E) instead of (r_i, s_i). But since user U_i knows the pair (r_i, s_i), he can, from it, construct a new pair (r'_i, s'_i) and use it to generate group signatures. This straight-forward application of the previously described forgery, however, does not work: the group authority will still be able to open the signature. But, as we can see, the process can be easily randomized:

(1) Randomly choose v ($\not\equiv 1 \pmod{q}$) and compute $\hat{\alpha}_i := {y_T}^{r_i}\, g^{s_i} \bmod p$ and $\alpha_i = ({\hat{\alpha}_i}^v)^a \bmod p$ for a randomly chosen a;
(2) Randomly choose w and set $\mu = ({\hat{\alpha}_i}^v)^w \bmod p$;
(3) Set $r'_{i,p} = \hat{\alpha}_i^{-v}\, \mu \bmod p$ and $r'_{i,q} = r_i\, v \bmod q$ and apply Chinese remaindering to $r'_{i,p}$ and $r'_{i,q}$ to obtain r'_i (see Eq. (3));
(4) Set $s'_i = s_i\, v \bmod q$;
(5) Choose a random b and compute $A = {r'_i}^a \bmod p$, $B = s'_i - b \bmod q$, $C = r'_i\, a \bmod q$, $D = g^a \bmod p$ and $E = g^{ab} \bmod p$;
(6) Compute $r = {\alpha_i}^t \bmod p$ for a randomly chosen t;
(7) Solve for s the congruence $h(m) \equiv st + wr \pmod{q}$;
(8) The Tseng-Jan group signature on message m is given by (r, s, A, B, C, D, E).

This group signature cannot be opened since $D^B\, {y_T}^C\, E \equiv (D^{k_i})^v \not\equiv D^{k_i} \pmod{p}$ (see Section 4). User U_i is thus able to produce *untraceable* (yet valid) group signatures. This forgery differs from the forgery against the Lee-Chang scheme in that it can only be mounted by group members. Furthermore, whereas the forgery against the Lee-Chang scheme is easily avoidable,[2] thwarting the previous attack in the Tseng-Jan scheme is not so obvious. The main problem is due to the fact that a malicious group member can "play" with his membership certificate, (r_i, s_i), to generate a fake (r'_i, s'_i). Moreover, since the values of r'_i and s'_i do not appear explicitly in the resulting group signatures, this malicious member may choose out of range values for r'_i and s'_i. This also means that making unlinkable the Lee-Chang scheme is certainly not an easy issue.

5.3 Universal forgeries

In § 5.1, we have shown that if the range conditions for (r_i, s_i) are not checked, anyone (not necessarily group member) can generate a Lee-Chang group signature which will be validated. In this paragraph, we show that, even if the range conditions are satisfied, it is still possible to generate a valid group signature in

[2] It suffices to check that the membership certificate (r_i, s_i) sent along with the group signature satisfies the range conditions $1 \leq r_i < p$ and $0 \leq s_i < q$.

the Lee-Chang scheme. Because the attack we present can be mounted equally well by a group member or by a non-group member, we call it *universal forgery*.

To forge a Lee-Chang group signature on a message m, we must find (r, s, r_i, s_i) such that (see Eq. (1))

$$\alpha_i{}^{h(m)} \equiv r^s \, DH_i{}^r \pmod{p}$$

with $\alpha_i = {y_T}^{r_i} \, g^{s_i} \bmod p$ and $DH_i = \alpha_i \, r_i \bmod p$. In this congruence, the values of α_i and DH_i are imposed —i.e., computed by the verifier from (r_i, s_i)— and so the apparent intractability to forge signatures. Suppose now that the representations of r and DH_i with respect to bases y_T and g are known. So let $r = {y_T}^v \, g^w \bmod p$ and $r_i = {y_T}^{v_i} \, g^{w_i} \bmod p$ (and hence $DH_i \equiv \alpha_i \, r_i \equiv {y_T}^{r_i + v_i} \, g^{s_i + w_i} \pmod{p}$) for some known v, w, v_i, w_i. The above congruence then becomes

$$({y_T}^{r_i} \, g^{s_i})^{h(m)} \equiv ({y_T}^v \, g^w)^s \, ({y_T}^{r_i + v_i} \, g^{s_i + w_i})^r \pmod{p}\,, \tag{4}$$

which is satisfied whenever

$$\begin{cases} r_i \, h(m) \equiv vs + (r_i + v_i)r \pmod{q} \\ s_i \, h(m) \equiv ws + (s_i + w_i)r \pmod{q} \end{cases}. \tag{5}$$

Therefore, an adversary can produce a valid Lee-Chang signature by carrying out the following steps:

(1) Randomly choose v, w, v_i and w_i;
(2) Compute $r = {y_T}^v \, g^w \bmod p$ and $r_i = {y_T}^{v_i} \, g^{w_i} \bmod p$;
(3) Solve for s the congruence $r_i \, h(m) \equiv vs + (r_i + v_i)r \pmod{q}$;
(4) Solve for s_i the congruence $s_i \, h(m) \equiv ws + (s_i + w_i)r \pmod{q}$;
(5) The Lee-Chang group signature on message m is given by (r, s, r_i, s_i).

A similar attack can also be mounted against the Tseng-Jan scheme but there is a simpler (universal) forgery. In the Tseng-Jan scheme, a group signature (r, s, A, B, C, D, E) must satisfy (see Eq. (2))

$$\alpha_i{}^{h(m)} \equiv DH_i{}^r \, r^s \pmod{p}$$

with $\alpha_i = D^B \, {y_T}^C \, E \bmod p$ and $DH_i = \alpha_i \, A \bmod p$. We first note that the value of α_i can be freely chosen if $E = \alpha_i \, (D^B \, {y_T}^C)^{-1} \bmod p$; likewise, the value of DH_i can be freely chosen if $A = DH_i \, {\alpha_i}^{-1} \bmod p$. Any adversary can thus computes a valid Tseng-Jan group signature as follows:

(1) Randomly choose r, ω, and compute $\alpha_i = r^\omega \bmod p$;
(2) Randomly choose B, C, D, and compute $E = \alpha_i \, (D^B \, {y_T}^C)^{-1} \bmod p$;
(3) Randomly choose σ and compute $DH_i = r^\sigma \bmod p$;
(4) Compute $A = DH_i \, {\alpha_i}^{-1} \bmod p$;
(5) Solve for s the congruence $\omega \, h(m) \equiv \sigma r + s \pmod{q}$;
(6) The Tseng-Jan group signature on message m is given by (r, s, A, B, C, D, E).

References

1. David Chaum and Eugène van Heijst. Group signatures. In *Advances in Cryptology — EUROCRYPT '91*, LNCS 547, pp. 257–265. Springer-Verlag, 1991.
2. Wei-Bin Lee and Chin-Chen Chang. Efficient group signature scheme based on the discrete logarithm. *IEE Proc. Comput. Digit. Tech.*, 145(1):15–18, 1998.
3. Anna Lysyanskaya and Zulfikar Ramzan. Group blind signatures: A scalable solution to electronic cash. In *Financial Cryptography (FC '98)*, LNCS 1465, pp. 184–197. Springer-Verlag, 1998.
4. Kaisa Nyberg and Rainer A. Rueppel. Message recovery for signature schemes based on the discrete logarithm problem. In *Advances in Cryptology — EUROCRYPT '94*, LNCS 950, pp. 182–193. Springer-Verlag, 1995.
5. Yuh-Min Tseng and Jinn-Ke Jan. Improved group signature scheme based on discrete logarithm problem. *Electronics Letters*, 35(1):37–38, 1999.