Improved Tseng-Jan’s group signature schemes 1)

Chunming Tang 2)Zhuojun Liu 3)Mingsheng Wang 4)

Abstract. The Tseng and Jan’s group signature scheme[1] is proven to be insecure[5].
In this paper, we improve it, and obtain a secure group signature scheme.

Keywords: Group signature; Cryptanalysis; Cryptography

1. Introduction

In 1999, Tseng and Jan proposed two improved group signature schemes([1, 2]), which are
based on the Lee-Chang scheme[3], called TJ1 and TJ2 schemes in this paper, respectively.
The improved TJ1 scheme is designed to avoid the cannotative linkage in the Lee-Chang
scheme. However, Sun showed in [4] that the scheme is still not unlinkable. Hence, Tseng
and Jan proposed TJ2 scheme to avoid the signature linkage[1]. In 2000, Zichen Li et al[5],
showed that both of TJ1 and TJ2 schemes are insecurity, that is, they can also produce a
valid group signature of TJ1 and TJ2 without knowing secret keys.

In this paper, we improve the TJ2 schemes, as a result, our scheme is secure even it is
attacked by the hacker similar to in [5].

2. Review of Tseng-Jan’s group signature schemes

Let $p$ and $q$ be large primes such that $q|p-1$, and let $g$ be a generator with order $q$ in
$GF(p)$.

Each group user $U_i$ holds the following keys:

$x_i : a$ secret key, $x_i \in Z_q^*$, $y_i : a$ public key, $y_i = g^{x_i} \mod p$.

The group authority $T$ has the following keys:

$x_T : a$ secret key, $x_T \in Z_q^*$, $y_T : a$ public key, $y_T = g^{x_T} \mod p$.

The group authority randomly chooses, for each group member $U_i$, an integer $k_i \in [1, q]$
and computes $r_i = g^{-k_i}y_i^{k_i} \mod p$, $s_i = k_i - r_ix_T \mod q$. $T$ then secretly sends $(r_i, s_i)$ to the
group member $U_i$.

For the message $m$, the group signature is $\{R, S, h(m), A, B, C, D, E\}$, where

$A = r_i^a \mod p$, $B = as_i - bh(A, C, D, E) \mod q$,

$C = r_ia - d \mod q$, $D = g^b \mod p$,

$E = y_d^2 \mod p$, $\alpha_i = g^B y_C^D E^D (A, C, D, E) \mod p$,

This work was supported in part by 973 project G1998030600.
2)ctang@mmrc.iss.ac.cn, Key Laboratory of Mathematics Mechanization, Institute of Systems Science,
Chinese Academy of Sciences, Beijing(100080)
3)zliu@zgc.gov.cn, Key Laboratory of Mathematics Mechanization, Institute of Systems Science, Chinese
Academy of Sciences, Beijing(100080)
4)mswang@is.iscas.ac.cn, State Key Laboratory of Information Security, Institute of Software, Chinese
Academy of Sciences, P.R.China
\[ R = \alpha_i^t \pmod{p}, \quad S = t^{-1}(h(m, R) - Rx_i) \pmod{q}, \]

\( h(\cdot) \) is one-to-one hash functions.

The integers \( a, b, d \) and \( t \) are randomly chosen from \( Z_q^* \) by \( U_i \).

Signature verification equation is:

\[ \alpha_i^{h(m, R)} = (\alpha_i A)^R R^S \pmod{p} \]  \hspace{1cm} (1)

3. Review of forgeable attacks on Tseng-Jan’s group signature schemes

In [5], Z.Li et al. proposed the forgery attack on the TJ2 signature schemes. That is, given any message \( m \), a hacker would produce the valid group signature without knowing the user’s secret key and \( (r_i, s_i) \).

**The attack on TJ2 scheme (ATJ2)**

The hacker chooses five pairs of random integers

\( (U_A, V_A), (U_C, V_C), (U_D, V_D), (U_E, V_E), (U_R, V_R) \)

in \( Z_q^* \), and computes:

\[ A = g^{U_A} y_T^V \pmod{p}, \]  \hspace{1cm} (2)
\[ D = g^{U_R} y_T^V \pmod{p}, \]  \hspace{1cm} (3)
\[ C = g^{U_C} y_T^V \pmod{p}, \]  \hspace{1cm} (4)
\[ E = g^{U_E} y_T^V \pmod{p}, \]  \hspace{1cm} (5)
\[ R = g^{U_R} y_T^V \pmod{p}, \]  \hspace{1cm} (6)

To simplify the notation, let \( H = h(A, C, D, E) \) and \( h = h(m, R) \). The hacker solves the following congruence equations to obtain values for the parameters \( B \) and \( S \).

\[ Bh + U_E h + U_D h = BR + U_E R + U_D HR + U_A R + U_R S \pmod{q} \]  \hspace{1cm} (7)
\[ Ch + V_E h + V_D h = CR + V_E R + V_D HR + V_A R + V_R S \pmod{q} \]  \hspace{1cm} (8)

The set \( \{R, S, m, A, B, C, D, E\} \) is a valid group signature forged by the hacker for message \( m \).

We have:

\[ \alpha_i = g^{B} y_T^C E D H = g^{B} y_T^C g^{U_E} y_T^V g^{U_D} H y_T^V \pmod{p}, \]
\[ \alpha_i A = g^{B} y_T^C g^{U_E} y_T^V g^{U_D} H y_T^V g^{U_A} y_T^V \pmod{p}, \]
\[ \alpha_i^h = g^{B h + U_E h + U_D H h} y_T^C g^{C R + V_E R + V_D H R} y_T^V \pmod{p}, \]
\[ (\alpha_i A)^R R^S = g^{BR + U_E R + U_D HR + U_A R + U_R S} g^{C R + V_E R + V_D HR + V_A R + V_R S} \pmod{p} \]

From equations (7) and (8), the signature verification equation \( \alpha_i^{h(m, R)} = (\alpha_i A)^R R^S \pmod{p} \) holds, so \( \{R, S, m, A, B, C, D, E\} \) is a valid group signature.
4. Improved Tseng-Jan’s group signature schemes

Before improving the TJ2 scheme, we first recall commitment schemes and some statistical zero-knowledge proofs of knowledge about modular relations based on the discrete logarithm.

4.1. Commitment scheme

In [7], Pederson proposed a computationally binding and unconditionally hiding scheme based on the discrete logarithm problem. The commitment scheme is following:

Given are a group $G$ of prime order $q$ and two random generator $g_1$ and $h$ such that $\log_{g_1}h$ is unknown and computing discrete logarithms is infeasible. A value $a \in \mathbb{Z}_q$ is committed to as $c_a := g_1^ah^r$, where $r$ is randomly chosen from $\mathbb{Z}_q$.

4.2. Zero-knowledge proofs of knowledge about some modular relations

In [6], Camenisch and Michels proposed some protocols in which the prover proves that the signature $S$ satisfies $d = \log_{g_1}h \mod q$, however, $S$ is only computed with $S_0$ without revealing any further information to the verifier, in particular, all protocols are statistical zero-knowledge. Three protocols are denoted by $S_+, S_-, S_{exp}$, respectively. In the following, we only list $S_+$ and $S_-$, however, $S_{exp}$ and all proofs are referred in [6].

Assume that the verifier has already obtained all commitments $c_a, c_b, c_d$ and $c_m$. Then $S_+$ and $S_-$ are following:

$$S_+ := PK\{(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta, \xi, \rho, \lambda) :$$

$$c_a = g_1^a h^\beta \cdot -2^l < \alpha < 2^l \land c_b = g_1^a h^\delta \cdot -2^l < \gamma < 2^l \land$$

$$c_a = g_1^a h^\gamma \cdot -2^l < \delta < 2^l \land c_m = g_1^a h^\rho \cdot -2^t < \eta < 2^t \land$$

$$\frac{c_a}{c_m} = c_d h^\lambda \cdot -2^t < \theta < 2^t \}$$

$$S_- := PK\{(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \theta, \xi, \rho, \sigma) :$$

$$c_a = g_1^a h^\beta \cdot -2^l < \alpha < 2^l \land c_b = g_1^a h^\delta \cdot -2^l < \gamma < 2^l \land$$

$$c_a = g_1^a h^\gamma \cdot -2^l < \delta < 2^l \land c_m = g_1^a h^\rho \cdot -2^t < \eta < 2^t \land$$

$$c_a = c_b \cdot c_d h^\sigma \cdot -2^l < \eta < 2^l \}$$

**Remark:** if $c_a, c_b, c_d, c_m$ satisfies $a^b = d \mod q$, we will denote it by $PK : (c_a = c_d\mod q) \in S_{exp}$. (if one or several integers are not committed, this integers will be denoted by $g_1^{integer}$ in the above equation. For example, given commitment $c_a, c_q$ and $b, d$, if they satisfy $a^b = d \mod q$, then, we denote zero-knowledge proof for it by $PK : (c_d = g_1^d (\mod q) \in S_{exp})$. In fact, the prover may first commit to $b, d$, she decommits the commitments $b, d$ after running $PK : (c_a = c_d\mod q) \in S_{exp}$.

4.3. Improved TJ2 scheme

From the TJ2 scheme, we can obtain the following equation:

$$C = r_i log_r A - log_{y_T} E \mod q. \quad (9)$$

So, if the signature $\{R, S, h(m), A, B, C, D, E, F\}$ is valid, $C$ is only computed with $r_i, A, y_T, E$.

In this scheme, $A, E, y_T$ are public, however, $r_i$ can’t be known by the illegal signer. Hence, in the signature procedure of the TJ2 scheme, if a zero-knowledge proof, in which the signer can prove that $C = r_i log_r A - log_{y_T} E \mod q$ holds for commitment $C_i$, without
revealing any information to any verifier, is run between the signer and the verifier, the ATJ2 can be avoided. According this ideal, we propose improved TJ2 group signature scheme.

Improved TJ2 scheme:

System initialization: The system parameters \((p, q, g, g_1, h)\), the secret keys \((x_i, x_T)\), the public \((y_i, y_T)\) and the parameters \((r_i, s_i)\) are similarly chosen as in TJ2, where \(g_1, h \in GF(p)\) are also generators with order \(q\) and \(log_q h\) is unknown for all members. At the same time, we commit to \(r_i\) with the commitment scheme in 4.1, and publish the commitment \(C_{r_i} = (g_1^{r_i}h^r)\), where \(r \in Z_q\) is random.

Signature procedure: For the message \(m\), the \(U_i\) constructs the group signature

\[
\{R, S, h(m), A, B, C, D, E, F, S_{proof}, C_e, C_f\},
\]

where the first six items are computed as in TJ2 scheme, \(S_{proof}\) denotes zero-knowledge proof for \(C = r_i log_r A - log_{y_T} E \pmod q\), and the \(C_e\) and \(C_f\) are commitments to \(log_r A\) and \(log_{y_T} E\), respectively. The detail protocol for \(S_{proof}\) is following:

\[
S_{proof} := PK \{ (\alpha, \beta, \gamma, \delta, \zeta, \eta, \mu, \nu) : \]

\[
C_{r_i} = g_1^{\alpha_1}h_1^{\beta} \land -2^l < \alpha < 2^l \land \quad (10)\]

\[
C_e = g_1^{\gamma_1}h_1^{\delta} \land -2^l < \gamma < 2^l \land \quad (11)\]

\[
(C_{r_i}^{C_e}) = A (mod q) \in S_{exp} \land \quad (12)\]

\[
C_f = g_1^{\zeta_1}h_1^{\eta} \land -2^l < \zeta < 2^l \land \quad (13)\]

\[
(C_{s_i}^{C_f}) = E (mod q) \in S_{exp} \land \quad (14)\]

\[
g_1^{\nu_1}h_1^{\mu} \land -2^l < \mu < 2^l \} \quad (15)\]

Remark: in (10)-(12), the prover proves that \(r_i^{\varphi} = A (mod q)\) holds; in (13)-(14), the prover proves that \(y_T^{\varphi} = E (mod q)\) holds; the prover proves that \(C = r_ie - f (mod q)\) holds in (15). Hence, the relation \(C = r_i log_r A - log_{y_T} E \pmod q\) holds.

Verification procedure: 1): \(\alpha_i^{h(m, R)} = (\alpha_iA)^{R}RS (mod p)\). 2) \(S_{proof}\) is real.

4.4. Security of improved TJ2 scheme

Because we do not change the TJ2 scheme, all good properties of TJ2 scheme are remained in our scheme. In the following, we mainly discuss how our scheme avoid the ATJ2.

By equation (8), we can obtain the following equation:

\[
C = (V_A R + V_R S)(h - R)^{-} - (V_E + V_D H) \pmod q
\]

Comparing between (9) and (16), the following equation is obtained:

\[
r_i log_r A - log_{y_T} E = (V_A R + V_R S)(h - R)^{-} - (V_E + V_D H) \pmod q
\]

Obviously, if the signer is legal, she can accurately run \(S_{proof}\) with the verifier for proving \(C = r_i log_r A - log_{y_T} E \pmod q\) with \(C_{r_i}, C_e, C_f\). Hence, his signature is valid. But, if the signer is illegal, he must forge \(r_i\) and provide \(C_{r_i}\) in the signature procedure, because he can not obtain the accurate \(r_i\), except that he can solve the following equation:

\[
A^{r_i} = r_i^{(V_A R + V_R S)(h - R)^{-} - (V_E + V_D H) + log_{y_T} E \pmod q}
\]
However, solving this equation is more difficult that doing the discrete logarithm problem. From the above discussion, the hacker can not obtain the accurate $r_i$ in the ATJ2, as a result, he can not run $S_{proof}$ with any verifier, so his signature is invalid.

At last, we must still prove that $S_{proof}$ is a zero-knowledge proof (in fact, it is a statistical zero-knowledge). This result can indirectly obtain from statistical zero-knowledge of $S_+, S_*, S_{exp}$.

So, we conclude that our improved TJ2 can avoid ATJ2.

Remark: In total paper, we do not improve the TJ1 scheme to avoid the attack in [5], this main reason is that the TJ1 is not unlinkable, obviously, it is not practical.

References


