# Untraceability of Wang-Fu Group Signature Scheme

Zhengjun Cao† Lihua Liu‡

†Center of Information Security, Academy of Mathematics and Systems Science,

Chinese Academy of Sciences, Beijing, P.R. China. 100080 zjcamss@hotmail.com

‡ Department of Mathematics, Shanghai Jiaotong University

**Abstract** Wang et al. recently proposed an improved edition based on Tseng-Jan group signature scheme[1]. In the paper, we show that the scheme is untraceable by a simple attack.

**Keywords** group signature scheme, full-anonymity, full-traceability.

## 1 Introduction

Group signatures, introduced by Chaum and Heyst[2], allow individual members to make signatures on behalf of the group. More formally, a secure group signature scheme must satisfy the following properties[6]:

- Unforgeability: Only group members are able to sign messages on behalf of the group.
- Anonymity: Given a valid signature of some message, identifying the actual signer is computationally hard for everyone but the group manager.
- Unlinkability: Deciding whether two different valid signatures were produced by the same group member is computationally hard.
- Exculpability: Neither a group member nor the group manager can sign on behalf of other group member.
- Traceability: The group manager is always able to open a valid signature and identify of the actual signer.
- Coalition-resistance: A colluding subset or group members (even if comprised of the entire group) cannot generate a valid signature that the group manager cannot link to one of the colluding group members.

The anonymity and traceability of group signature scheme make it very useful in E-commerce activities[3,4].

Lee and Chang proposed a group signature in 1998[5], but it has serious drawbacks. Hence, Tseng and Jan proposed two improved group signature schemes based on Lee-Chang scheme. Regrettably, their schemes are all insecure, too. Z.C.Li et al. have presented several attacks on them[7,8,9,10,11,12,13]. Incidentally, We have given a new and simple attack in a script.

Recently, Wang and Fu proposed a new edition based on Tseng-Jan scheme. In this paper, we show that the new edition is also insecure by a simple attack. It shows that Wang-Fu group signature scheme is untraceable.

# 2 Wang-Fu group signature scheme

## 2.1 Setup

(1) Pick two large primes $p, q$, such that $q|(p-1)$, $g \in GF(p)$ is a generator of order $q$. Open $p, q, g$ as public parameters.

(2) Member $u_i$ randomly chooses secret key $x_i \in Z_q^*$, computes public key $y_i = g^{x_i}\ (mod\ p)$. Group manager $T$ randomly chooses secret key $x_T \in Z_q^*$, computes public key $y_T = g^{x_T}\ (mod\ p)$.

(3) Choose a secure Hash function $h$.

## 2.2 Join

When $u_i$ join the group, he executes as follows:

(1) $T$ randomly picks $k_i \in Z_q^*$, computes

$$r_i = g^{-k_i} y_i^{k_i}\ (mod\ p), \qquad s_i = k_i - r_i x_T\ (mod\ q)$$

sends $s_i, r_i$ to $u_i$ in secret, keeps $(s_i, r_i, k_i)$ in record.

(2) After $u_i$ receives $(s_i, r_i)$, he verifies

$$g^{s_i} y_T^{r_i} r_i \stackrel{?}{=} (g^{s_i} y_T^{r_i})^{x_i}\ (mod\ p)$$

If it holds, $u_i$ accepts $(s_i, r_i)$.

### 2.3 Sign

Given a message $m$, $u_i$ randomly chooses $a, b, d, t \in Z_q^*$, computes

$$\begin{aligned}
C &= r_i a - d \ \ (mod\ q), \\
A &= y_i^b \ \ (mod\ p), \\
D &= g^b \ \ (mod\ p), \\
E &= r_i^a (1 + g^{-s_i a} y_T^{-r_i a})^{x_i} \ \ (mod\ p), \\
F &= y_T^d \ \ (mod\ p), \\
B &= s_i a - bh(A, C, D, E, F) + bh(E, D, F) \ \ (mod\ q), \\
\alpha_i &= [D^{h(E,D,F)} + g^B y_T^C F D^{h(A,C,D,E,F)}] \ \ (mod\ p), \\
R &= \alpha_i^t \ \ (mod\ p), \\
s &= t^{-1}[h(m, R) - x_i R] \ \ (mod\ q).
\end{aligned}$$

The signature is $(s, R, A, B, C, D, E, F, m)$.

### 2.4 Verify

Verifier computes

$$\begin{aligned}
\alpha_i &= D^{h(E,D,F)} + g^B y_T^C F D^{h(A,C,D,E,F)} \ (mod\ p), \\
\delta_i &= A^{h(E,D,F)}[\alpha_i D^{-h(E,D,F)} - 1]E \ (mod\ p)
\end{aligned}$$

Check

$$\alpha_i^{h(m,R)} \stackrel{?}{=} \delta_i^R R^s \ (mod\ p)$$

If it holds, then $(s, R, A, B, C, D, E, F, m)$ is a valid group signature.

### 2.5 Open

Group Manager $T$ who knows $(s_i, r_i, k_i)$ of member $u_i$, $(i = 1, 2, \cdots, n.)$ computes

$$v_i = s_i^{-1} k_i \ (mod\ q), \qquad \omega_i = g^{v_i} \ (mod\ p)$$

and checks

$$g^B y_T^C F D^{h(A,C,D,E,F)} = \omega_i^B D^{[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]} \ (mod\ p)$$

Therefore, he can reveal the signer of $(s, R, A, B, C, D, E, F, m)$.

### 2.6 Delete member

Omitted.

## 3 Untraceability

In recent, Bellare et al. have pointed out that full-anonymity and full-traceability are two basic requirements of group signature, one can refer to [6] or [14] for more details. Without question, it is an excellent explanation after the concept of group signature has been invented. But we find that the improved scheme is untraceable although it overcomes some drawbacks of original scheme.

**Attack:**

Given a message $m$, member $u_i$ randomly picks $a, b, d, t \in Z_q^*$, $\underline{\rho \in Z_q^*}$, computes

$$\begin{aligned}
C &= r_i a - d \ \ (mod\ q), \\
A &= y_i^b \ \ (mod\ p), \\
D &= g^b \ \ (mod\ p), \\
E &= r_i^a(1 + g^{-s_i a} y_T^{-r_i a})^{x_i} \ \ (mod\ p), \\
\hat{F} &= y_T^d \underline{g^\rho} \ \ (mod\ p), \\
\hat{B} &= s_i a - bh(A, C, D, E, \hat{F}) + bh(E, D, \hat{F}) \underline{-\rho} \ \ (mod\ q), \\
\alpha_i &= [D^{h(E,D,\hat{F})} + g^B y_T^C \hat{F} D^{h(A,C,D,E,\hat{F})}] \ \ (mod\ p), \\
R &= \alpha_i^t \ \ (mod\ p), \\
s &= t^{-1}[h(m, R) - x_i R] \ \ (mod\ q).
\end{aligned}$$

The group signature is $(s, R, A, \hat{B}, C, D, E, \hat{F}, m)$.

**Correctness:** Since

$$\begin{aligned}
\alpha_i &= D^{h(E,D,\hat{F})} + g^{\hat{B}} y_T^C \hat{F} D^{h(A,C,D,E,\hat{F})} \\
&= g^{bh(E,D,\hat{F})} + g^{s_i a} g^{-bh(A,C,D,E,\hat{F})} g^{bh(E,D,\hat{F})} \underline{g^{-\rho}} g^{x_T r_i a} g^{-x_T d} g^{x_T d} \underline{g^\rho} g^{bh(A,C,D,E,\hat{F})} \\
&= g^{bh(E,D,\hat{F})}(1 + g^{s_i a} g^{x_T r_i a}) = g^{bh(E,D,\hat{F})}(1 + g^{k_i a}) \qquad (mod\ p) \\
\delta_i &= A^{h(E,D,\hat{F})}[\alpha_i D^{-h(E,D,\hat{F})} - 1]E \ (mod\ p)
\end{aligned}$$

we have

$$
\begin{aligned}
\alpha_i^{H(m,R)} &= \alpha_i^{x_i R}\alpha_i^{ts} = [g^{bh(E,D,\hat{F})x_i} g^{k_i a x_i}(1+g^{-k_i a})^{x_i}]^R R^s \\
&= [A^{h(E,D,\hat{F})} g^{k_i a} r_i^a (1+g^{-s_i a} y_T^{-r_i a})^{x_i}]^R R^s \\
&= [A^{h(E,D,\hat{F})} (\alpha_i g^{-bh(E,D,\hat{F})}-1) r_i^a (1+g^{-s_i a} y_T^{-r_i a})^{x_i}]^R R^s \\
&= \delta_i^R R^s \qquad (mod\ p)
\end{aligned}
$$

But

$$
g^{\hat{B}} y_T^C \hat{F} D^{h(A,C,D,E,\hat{F})} = g^{k_i a} g^{bh(E,D,\hat{F})} \quad (mod\ p)
$$

$$
\begin{aligned}
& \omega_i^{\hat{B}} D^{[h(A,C,D,E,\hat{F})v_i - h(E,D,\hat{F})v_i + h(E,D,\hat{F})]} \\
= \ & (g^{s_i^{-1}k_i})^{[s_i a - bh(A,C,D,E,\hat{F}) + bh(E,D,\hat{F}) \underline{-\rho}]} g^{bh(A,C,D,E,\hat{F})s_i^{-1}k_i} g^{-bh(E,D,\hat{F})s_i^{-1}k_i} g^{bh(E,D,\hat{F})} \\
= \ & g^{k_i a} g^{bh(E,D,\hat{F})} \underline{\omega_i^{-\rho}} \quad (mod\ p)
\end{aligned}
$$

$$
g^{\hat{B}} y_T^C \hat{F} D^{h(A,C,D,E,\hat{F})} \neq \omega_i^{\hat{B}} D^{[h(A,C,D,E,\hat{F})v_i - h(E,D,\hat{F})v_i + h(E,D,\hat{F})]} \quad (mod\ p)
$$

It means that the scheme is untraceable. ( Underlined parts show the differentia between the attack and the original scheme!! )

**Remark** The two attacks presented in [7] on original Tseng-Jan group signature scheme are applied to the new edition. But our attack is more simple because it only needs to choose another random number $\rho$.

## 4 Conclusion

In the paper, we analyze Wang-Fu group signature scheme, and show its untraceability by a simple attack. We hold that the structure of Tseng-Jan group signature is too loose to withstand any attacks. Various editions of the scheme have been studied in [7, 8, 9, 10, 11, 12, 13]. It's easy to see that the scheme has no any specialities whether in setup phase or in open phase. So, we think that it's no necessary to make any improvements of it.

## References


[1] Xiaoming Wang, Fangwei Fu. A Secure Group Signature Scheme. Journal of Elecetronics and Information (in Chinese), 2003 Vol.25 No.5. pp.657-663.

[2] D.Chaum, F.Heyst. Group Signatures. Proc. EUROCRYPT'91, 1992, pp.257-265.

[3] G. Maitland and C. Boyd. Fair electronic cash based on a group signature scheme In: Information Security and Cryptography (ICICS 2001), LNCS 2229, pp. 461-465, Springer-Verlag: 2001.

[4] S. Canard and J. Traore. On Fair E-cash Systems Based on Group Signature Schemes. In: Information Security and Privacy (ACISP'03), LNCS 2727, pp. 237-248. Berlin: Springer-Verlag, 2003.

[5] W.Lee, C. Chang. Efficient Group Signature Scheme Based on the Discrete Logarithm. IEE Pro. Comput. Digital Techniques. 1998, 145(1), pp.15-18.

[6] M. Bellare, D. Micciancio, B. Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. EUROCRYPT 2003. LNCS 2656, pp.614-629, 2003.

[7] Guilin Wang. Security of Several Group Signature Schemes. http://eprint.iacr.org/2003/194.

[8] Z.C.Li, L.C.K.Hui, et al. Security of Tseng-Jan's Group Signature Schemes. Information Processing Letters, 2000, 75(5), 187-189.

[9] M. Joye, N-Y. Lee, and T. Hwang. On the security of the Lee-Chang group signature scheme and its derivatives. In: Information Security (ISW'99), LNCS 1729, pp. 47-51. Springer-Verlag, 1999.

[10] H. Sun. Comment: Improved group signature scheme based on discrete logarithm problem. Electronics Letters, 1999, 35(13): 1323-1324.

[11] Y.-M. Tseng and J.-K. Jan. Improved group signature scheme based on the discrete logarithm problem. Electronics Letters, 1999, 35(1): 37-38.

[12] Y.-M. Tseng and J.-K. Jan. Reply: improved group signature scheme based on discrete logarithm problem. Electronics Letters, 1999, 35(13): 1324-1325.

[13] Guilin Wang and Sihan Qing. Security Flaws in Several Group Signatures Proposed by Popescu. Cryptology ePrint archive, report 2003/207, Sep 2003. http://eprint.iacr.org/2003/207.

[14] Mihir Bellare and Haixia Shi and Chong Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. http://eprint.iacr.org/2004/077.