Journal of Zhejiang University SCIENCE
ISSN 1009-3095
http://www.zju.edu.cn/jzus
E-mail: jzus@zju.edu.cn

**Discussion:**

# Colluding attacks on a group signature scheme*

GUO Xing-yang (郭兴阳)†[1,2], TANG Chao-jing (唐朝京)†[1]

([1]*School of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China*)

([2]*School of Telecommunication Engineering, Air Force Engineering University, Xi'an 710077, China*)

†E-mail: saga_gxy@sina.com; cjtang@263.net

Received June 10, 2005; revision accepted Sept. 5, 2005

**Abstract:** Xie and Yu (2005) proposed a group signature scheme and claimed that it is the most efficient group signature scheme so far and secure. In this paper, we show that two dishonest group members can collude to launch two attacks on the scheme. In the first attack they can derive the group secret key and then generate untraceable group signatures. In the second attack, they can impersonate other group members once they see their signatures. Therefore we conclude that the signature scheme is not secure. We show that some parameters should be carefully selected in the scheme to resist our attacks.

**Key words:** Group signature, Colluding attack, Factoring problem
**doi:**10.1631/jzus.2005.A1011 **Document code:** A **CLC number:** TP309

## INTRODUCTION

The concept of group signature, first introduced by Chaum and van Heyst (1992), allows each group member (and only the group member) to sign messages on behalf of the group, and requires that the receiver can use a group public key to verify the group signature, but cannot reveal the signer. The group signature should be traceable, i.e. the group authority can open the group signature and identify the signer. The outsider cannot identify all previous group signatures generated by the same group member. A group member cannot impersonate another group member and forge a valid signature by colluding with the group authority or other group members.

Xie and Yu (2005) proposed a novel group signature scheme with one time secret key. They claimed that their scheme is more efficient compared with that proposed by Ateniese *et al*.(2000) and that their scheme satisfies the security requirements of group signatures. But unfortunately, their claim is not true. We find that two dishonest group members can collude to derive the group secret key and then generate untraceable group signatures, and impersonate another group member once they see one signature of the member. In this paper we review the original signature scheme and then demonstrate two attacks on it.

## REVIEW OF XIE-YU SCHEME

The scheme involves four parties: the trusted center, the group authority, the group members and the verifier. The scheme consists of four phases: the system initialization phase, the partial secret key generation phase, the group signature generation and verification phase, and the signer identity verification phase.

### System initialization phase

The trusted center chooses four large primes: $p$, $q$, $p'$ and $q'$, such as $p=2p'+1$, $q=2q'+1$, and computes $N=pq$. Let $g$ be a generator of a multiplicative subgroup of $Z_N^*$ with order $v=p'q'$. Randomly chooses $e$ such that $gcd(e,v)=1$, and computes $d$ from $ed=1 \bmod v$. Let $h()$ be a one-way collision resistant crypto-

* Project (No. 60472032) supported by the National Natural Science Foundation of China

graphic hash function. The trusted center selects group secret key $x$, and computes group public key $y=g^x \bmod N$. Then, the trusted center publishes $e$, $y$, $N$, $g$ and $h()$, and keeps $p$, $q$, $p'$, $q'$, $d$, $x$ and $v$ secret.

**Partial secret key generation phase**

Let $A=\{U_1,U_2,\ldots,U_n\}$ be the group of $n$ members. The trusted center randomly selects $x_G$ as the group authority's secret key. For each group member $U_i \in A$, chooses a large prime $ID_i$ as $U_i$'s secret identity information, and computes $U_i$'s partial secret key $x_i=ID_i x d \bmod v$, the signer $U_i$'s identity verification parameter $T_i = g^{ID_i^{-1}} \bmod N$, $U_i$'s public key $y_i = T_i^{x_G} \bmod N$, and the group authority's public key $y_G = g^{x_G} \bmod N$.

Then, the trusted center sends $\{x_i, T_i, ID_i\}$ to each $U_i$, and sends $\{x_G, T_i\}$ to the group authority via a secure channel, respectively. After that, the trusted center publishes each group member's public key $y_i$ and the group authority's public key $y_G$.

**Group signature generation and verification phase**

Assuming that the member $U_i$ wants to sign a message $m$ on behalf of the group, he performs the following steps to generate the group signature:

(1) Randomly chooses a large prime $k$, computes $z=kID_i$, $r=g^k \bmod N$, and his secret key $s_i=x_i k$;

(2) Computes $c=h(r^e \bmod N, z, r, m)$, $s=k-s_i c$, $A = T_i^c \bmod N$;

(3) Sends the group signature $\{c, s, z, r, A\}$ to the verifier.

The verifier can use the group public key $y$ to authenticate whether the group signature $\{c, s, z, r, A\}$ of a message $m$ is valid or not as follows:

(1) Computes $R = g^{se} y^{zc} \bmod N$;

(2) Verifies the following equations:

$$c=h(R, z, r, m),\ R=r^e \bmod N,\ A^z=r^c \bmod N.$$

If all the above equations hold, then the group signature is verified.

**Signer identity verification phase**

In case of disputes later, the group authority can open the signature by checking which $T_i$ satisfies the equation:

$$T_i^z = r \bmod N.$$

In order to convince other verifiers that the user $U_i$ with the public key $y_i$ is indeed the actual signer, the group authority randomly chooses an integer $k_G$, and computes:

$$r_G = T_i^{k_G} \bmod N,\ s_G = x_G r_G + c k_G.$$

Then the group authority publishes the identification information $(r_G, s_G)$ and the $U_i$'s public key $y_i$. The verifier may identify $U_i$ with $y_i$ for the group signature $\{c, s, z, r, A\}$ by checking the following equation:

$$y_i^{z r_G} r_G^{cz} = r^{s_G} \bmod N.$$

If the above equation holds, the user with the public key $y_i$ is identified.

## SECURITY ANALYSIS OF XIE-YU SCHEME

We assume that there exist two dishonest group members $U_1$ and $U_2$ in the group. In the following we demonstrate an attack such that they can derive the group secret key kept secretly by the trusted center and then generate group signatures that the group authority cannot open to identify the signer. The second attack is partially based on the first attack. With the secret key of the trusted center, the two colluding group members can impersonate any other group member once they see one of his signatures.

**Attack 1**

Step 1: $U_1$ and $U_2$ reveal their identity information $ID_1$ and $ID_2$ to each other.

Step 2: $U_1$ computes $\delta_1 = ID_2 x_1 e$.

Because $ed=1 \bmod v$ and $x_1=ID_1 x d \bmod v$, we assume that

$$ed=1+av,\ x_1=ID_1 x d-b_1 v.$$

Then we can see that

$$\begin{aligned}\delta_1 &= ID_2\, x_1 e \\ &= ID_2\,(ID_1 x d - b_1 v)e \\ &= ID_2\,(ID_1 x d e - b_1 e v)\end{aligned}$$

$$=ID_2ID_1xde-ID_2b_1ev$$
$$=ID_2ID_1x(1+av)-ID_2b_1ev$$
$$=ID_2ID_1x+ID_2ID_1xav-ID_2b_1ev$$
$$=ID_2ID_1x+(ID_2ID_1xa-ID_2b_1e)v.$$

Step 3: Similarly, $U_2$ computes

$$\delta_2=ID_1x_2e=ID_1ID_2x+(ID_1ID_2xa-ID_1b_2e)v.$$

Step 4: $U_1$ and $U_2$ Compute

$$\delta=\max(\delta_1, \delta_2)-\min(\delta_1, \delta_2).$$

We assume that $\delta_1>\delta_2$, Then

$$\delta=\delta_1-\delta_2=(ID_1b_2-ID_2b_1)ev.$$

Step 5: $U_1$ and $U_2$ factor the modulus $N$ with $\delta$ and derive $p$ and $q$.

It is well known that knowing $\delta$, a non-zero multiple of $v$, the modulus $N$ can be easily factored (Koblitz, 1994). Some researchers (Dodis and Reyzin, 2003; Wang *et al.*, 2004) have shown that this problem should not be ignored when researchers design cryptographic schemes. We will show why $\delta$ is a non-zero value latter.

Step 6: $U_1$ and $U_2$ compute $v=(p-1)(q-1)/4$. Then they compute $d$ such that $ed=1 \bmod v$ and

$$x_v=ID_i^{-1}x_ie \bmod v=x \bmod v.$$

Step 7: $U_1$ and $U_2$ randomly choose a large prime $ID'$ and compute

$$x'=ID'\, x_vd \bmod v=ID'\, xd \bmod v,\ T'=g^{ID'^{-1}} \bmod N.$$

Step 8: $U_1$ and $U_2$ generate a group signature with the partial secret key $(x',T',ID')$.

Obviously, they can generate a valid group signature with $(x',T',ID')$. When the group authority opens the group signature, it cannot find $T'$ in its database which satisfies the equation:

$$T'^{\,z}=r \bmod N.$$

**Attack 2**

$U_1$ and $U_2$ derive $v$, $x_v$ and $d$ as in Attack 1. When they see a group signature $\{c, s, z, r, A\}$ generated by another group member $U_i$, they can impersonate him to generate a group signature as follows:

Step 1: Compute

$$k'= s+z\, x_v\, dc \bmod v$$
$$=s+kID_ixdc \bmod v$$
$$=s+kx_ic \bmod v$$
$$=s+s_ic \bmod v$$
$$=k \bmod v.$$

Step 2: Compute

$$ID_i'=zk'^{\,-1} \bmod v=k\, ID_i\, k^{-1} \bmod v=ID_i \bmod v.$$

Step 3: Compute

$$X_i=ID_i'x_v\, d \bmod v=ID_ixd \bmod v.$$

Step 4: Compute

$$T_i=g^{ID_i'^{-1}} \bmod N=g^{ID_i^{-1}} \bmod N.$$

Step 5: $U_1$ and $U_2$ generate a group signature with the partial secret key $(x_i,T_i,ID_i')$.

We can easily see that $ID_i'$ may not be equal to $ID_i$, but that the group signature generated with $(x_i,T_i, ID_i')$ is always valid and the group authority will identify the signer as $U_i$.

**Discussion on parameters selection**

In Step 5 of Attack 1, $U_1$ and $U_2$ must derive a non-zero value $\delta$. Otherwise the attack will fail. In the following we show why $\delta$ is not zero.

We assume $\delta=0$ for any two group members $U_1$ and $U_2$, then

$$ID_2\, x_1e=ID_1x_2e.$$

We derive that

$$\frac{ID_1}{ID_2}=\frac{ID_1xd \bmod v}{ID_2xd \bmod v} \quad \text{in } Z.$$

Since $ID_i$ is prime number, $ID_i$ must be less than $v$ and we have

$$ID_ixd \bmod v=n'ID_i \tag{1}$$

Here $n'$ will be a constant, therefore

$$ID_ixd-b_iv=n'ID_i$$

and then

$$xd=(b_i/ID_i)v+n' \quad (2)$$

If Eq.(2) does not hold, $\delta\neq 0$. Therefore to ensure that Eq.(2) holds to resist the attacks, the trusted center must select $n'$, $(b_i/ID_i)$ and $x$ carefully. It should be noticed that $(b_i/ID_i)$ is also a constant. At the same time, to ensure that Eq.(1) holds, $n'$ must be as small as possible to leave enough value space to select $ID_i$. In the original paper, the two parameters $n'$ and $(b_i/ID_i)$ are not specified and $ID_i$ and $x$ are apparently selected randomly.

## CONCLUSION

In this paper, we demonstrated two attacks on the Xie-Yu group signature scheme which is a more efficient group signature scheme than all previous proposals but unfortunately, is not secure. We show the limitation in selecting some parameters in the scheme to resist our attacks. In fact, how to design a secure and efficient group signature scheme is still a hot topic.

## References

Ateniese, G., Camenisch, J., Joye, M., Tsudik, G., 2000. A Practical and Provably Secure Coalition-resistant Group Signature Scheme. CRYPTO 2000, LNCS1880, Springer-Verlag, Berlin, p.255-270.

Chaum, D., van Heyst, E., 1992. Group Signatures. Eurocrypt'91, LNCS547, Springer-Verlag, Berlin, p.257-265.

Dodis, Y., Reyzin, L., 2003. Breaking and Repairing Optimistic Fair Exchange from PODC 2003. Proceedings of ACM Workshop on Digital Rights Management, ACM Press, New York, p.47-54.

Koblitz, N., 1994. A Course in Number Theory and Cryptography (2nd Ed.). Springer-Verlag, New York.

Wang, G.L., Bao, F., Zhou, J.Y., Deng, R.H., 2004. Comments on "A practical (*t*, *n*) threshold proxy signature scheme based on the RSA cryptosystem". *IEEE Transactions on Knowledge and Data Engineering*, **16**(10):1309-1311.

Xie, Q., Yu, X.Y., 2005. A novel group signature with one time secret key. *Journal of Zhejiang University SCIENCE*, **6A**(6):560-564.