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

# A novel group signature with one time secret key*

XIE Qi (谢 琪)†1,2, YU Xiu-yuan (于秀源)3,4

(1Department of Mathematics, Zhejiang University, Hangzhou 310027, China)
(2School of Information and Engineering, Hangzhou Teachers College, Hangzhou 310012, China)
(3Department of Mathematics, Hangzhou Teachers College, Hangzhou 310012, China)
(4Department of Mathematics and Physics, Quzhou College, Quzhou 324000, China)
†E-mail: qixie68@yahoo.com.cn; qixie@hztc.edu.cn

Received Mar. 10, 2004; revision accepted Sept. 20, 2004

**Abstract:** A new group signature with one time secret key is proposed. The main merits are that it only needs the trusted center issuing the partial secret key one time for each group member; and that the group member can generate his different secret key each time when he wants to sign a message. The group public key is constant and the size of the signature is independent of the number of group members. The total computation cost of signature and verification requires only 8 modular exponentiations.

**Key words:** Cryptography, Group signature, Discrete logarithm problem, Factoring problem
**doi:**10.1631/jzus.2005.A0560 **Document code:** A **CLC number:** TP309

## INTRODUCTION

The concept of group signature, first introduced by Chaum and van Heyst (1992), allows each group member to sign messages on behalf of the group, and the receiver can use a group public key to verify the group signature, but cannot reveal the signer. In case of disputes, the group authority can open the group signature and identify the signer, but 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.

Since Chaum and van Heyst proposed the first interactive group signature, some non-interactive group signatures and their improvement schemes were proposed. For example, convertible group signature (Kim *et al*., 1996), ID-based group signature (Park *et al*., 1997; Tseng and Jan, 1998; 1999a; 1999b; Popescu, 2000; 2002), group signature scheme based on self-certified public keys (Tseng and Jan, 1999c), group signature scheme with strong separability (Xia and You, 2002), and group signature scheme with forward security (Song, 2001; Zhang *et al*., 2003). However, almost all secure group signature schemes are not very efficient (Wang, 2003a), and all efficient group signature schemes proposed so far are proved insecure (Sun, 1999; Wang *et al*., 1999; Joye *et al*., 1999a; 1999b; Li *et al*., 1999; Saeednia, 2000; Wang, 2003a; 2003b; 2004), the schemes exhibit some or one of the following shortcomings: universal forgery, linkability, untraceability, coalition attacks etc.

Zhang *et al*.(2003) proposed a very efficient forward-secure group signature scheme. The total computation cost of signature and verification requires only 7 modular exponentiations, while 36 modular exponentiations are needed in Song's scheme. However, Wang (2004) showed that Zhang *et al*.'s scheme is linkable, untraceable and forgeable by presenting several attacks on them. The current state of the art is proposed by Ateniese *et al*.(2000), whose scheme is the most efficient one and provably secure. Unfortunately several limitations still render

* Project (No. 10271037) supported by the National Natural Science Foundation of China

all previous group signature schemes unsatisfactory in practice. Hence group signatures remain in the domain of theoretical results.

In this paper, we present a novel group signature with one time secret key. The main merits are that it only needs the trusted center issuing the partial secret key one time for each group member; and that the group member can generate his different secret key each time when he wants to sign a message. The group public key is constant and the size of the signature is independent of the number of group members. The total computation cost of signature and verification requires only 8 modular exponentiations. The security of the proposed scheme is based on the difficulties of the discrete logarithm problem and the factoring problem.

## THE PROPOSED SCHEME

The proposed scheme involves four parties: the trusted center, responsible for choosing the system parameters and the group member's partial secret key; the group authority, who opens the group signature to find who the signer is in case of disputes later; the group members, who generate the signature on behalf of the group anonymously; the verifier, who uses the group public key to authenticate the validity of the group signature.

Our 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 choose $e$ such that $gcd(e, v)=1$, and compute $d$ from $ed=1 \bmod v$. Let $h()$ be a one-way collision resistant cryptographic 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. For each group member $U_i\in A$, the trusted center randomly selects $x_G$ as the group authority's secret key, and chooses a large prime $ID_i$ as $U_i$'s secret identity information, and computes $U_i$'s partial secret key $x_i=ID_i xd \bmod v$, 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 $y_G$. On receiving the secret information $\{x_i, T_i, ID_i\}$, each $U_i$ can authenticate whether $\{x_i, T_i, ID_i\}$ is valid or not by checking the equations:

$$T_i^{x_i e}=g^x=y \bmod N, \quad y_i^{ID_i}=T_i^{x_G ID_i}=y_G \bmod N.$$

### 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 $s_i=x_ik$;

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

(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:

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

The correctness of the above equation can be easily seen as follows:

$$R=g^{se}y^{zc}=g^{se+xkID_icde}=g^{(s+kx_ic)e}=g^{(s+s_ic)e}$$
$$=g^{ke}=r^e \bmod N.$$
$$A^z=T_i^{cz}=g^{ID_i^{-1}kID_ic}=g^{kc}=r^c \bmod N.$$

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

### The signer identity verification phase

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

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

The correctness of the above equation can be easily seen as:

$$T_i^z = g^{ID_i^{-1}kID_i} = g^k = r \bmod N.$$

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:

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

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:

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

If the above equation holds, the user with the public key $y_i$ is identified. The correctness of the above equation can be seen as follows:

$$y_i^{zr_G} r_G^{cz} = T_i^{x_G zr_G + k_G cz} = T_i^{zs_G} = r^{s_G} \bmod N.$$

## SECURITY ANALYSIS

In this section, we will discuss the security of the proposed scheme, and will show that it is secure.

1. No one can obtain the secret parameters

If the attacker (or group member) wants to know the group secret key $x$ from $y=g^x \bmod N$, or to find $d$ with the known $e$, he will encounter the difficulties of the discrete logarithm problem, or the factoring problem. On the other hand, since the trusted center keeps $v$ secret, therefore, each group member cannot know $x$, $d$ or $xd$ from $x_i=ID_ixd \bmod v$. The attacker knows that obtaining ($k$, $s_i$) from $s=k-s_ic$ is infeasible, because of the intractability of solving the bivariate simple equation.

2. The attacker cannot identify all previous group signatures generated by the same group member even if one group signature is identified

The proposed scheme has the property of one-time pad. That is, when a group member wants to sign a message, he will generate a new secret key $s_i=x_ik$ according to the partial secret key $x_i$. Since $z=kID_i$ is chosen to be impossible to factor, the attacker does not obtain $k$ and $ID_i$. Moreover, even if the group authority publishes the identification information ($r_G$, $s_G$), the anonymity of $U_i$'s previous signatures is not damaged. The reason is that the information ($r_G$, $s_G$) is only provided for the specific group signature $\{c, s, z, r, A\}$. Therefore, the attacker cannot identify all previous group signatures generated by the same group member even if one group signature is identified.

3. All group members cannot produce valid group signature that is untraceable by the group authority

To achieve the aim of untraceability, the group member may choose the following approach to generate the group signature.

He chooses two random large primes $k$ and $k'$ and computes

$$z = kID_i,\ r' = g^{k'} \bmod N,\ s_i = x_ik,$$
$$c' = h((r')^e \bmod N, z, r', m),\ s' = k' - s_ic',$$
$$A' = T_i^{c'} \bmod N.$$

Then he sends the group signature $\{c', s', z', r', A'\}$ to the verifier.

The verifier computes $R' = g^{s'e} y^{zc'} \bmod N$, and checks if $c' = h(R', z, r', m)$, $R' = (r')^e \bmod N$, $(A')^z = (r')^{c'} \bmod N$ or not. However, the equation $(A')^z = (r')^{c'} \bmod N$ cannot feasibly be solved.

Since the signature messages {$c$, $s$, $z$, $r$, $A$} are tightly co-related, the proposed scheme is secure.

4. The proposed scheme can resist conspiracy attack and forgery attack

If the group member $U_j$ has the signature {$c$, $s$, $z$,

$r$, $A$} of a message $m$ generated by $U_i$, and wants to impersonate $U_i$ to forge a valid group signature for the message $m'$, he may compute

$$z' = zID_j = kID_iID_j, \quad r' = r^{ID_j} = g^{kID_j} \bmod N,$$
$$s_j = x_j z, \quad c' = h((r')^e \bmod N, z', r', m'),$$
$$s' = kID_j - s_j c', \quad A' = T_j^{c'} \bmod N.$$

$\{c', s', z', r', A'\}$ is the group signature. However, the group member $U_j$ cannot compute $s'=kID_j-s_jc'$ because he does not know $k$ or $kID_j$ from $z=kID_j$ or $r' = g^{kID_j} \bmod N$.

If the group member $U_i$ colludes with the group authority, the group authority tries to publish the $U_j$'s identification information ($r_G$, $s_G$) for the group signature $\{c, s, z, r, A\}$ generated by $U_i$ as follows:

Randomly chooses an integer $k_G$, and computes

$$r_G = T_j^{k_G} \bmod N, \quad s'_G = x_G r_G + ck_G,$$

then he finds $s_G = ID_j^{-1} ID_i s'_G$ such that

$$T_j^{zs'_G} = r^{s_G} \bmod N.$$

However, it is infeasible because neither the group member $U_i$ nor the group authority knows the $U_j$'s $ID_j^{-1}$. That is, the proposed scheme can resist conspiracy attack.

## EFFICIENCY ANALYSIS

The computational cost and signature size play a determinating role in the performance efficiency. In this section, we compare our scheme with that in Ateniese *et al*.(2000)'s in terms of both computational cost and signature size.

In a signature scheme, the computational cost of signature is mainly determined by modular exponentiation and hash. Let $E$ and $H$ denote the computation load for modular exponentiation and hash, respectively. In our scheme, the total computation cost of signature and verification requires $8E+2H$. In the Ateniese *et al*.(2000)'s scheme, the total computation cost of signature and verification requires $23E+2H$.

On the other hand, assume that the system parameters $p$, $q$, $p'$ and $q'$ in our scheme are the same as that of the Ateniese *et al*.'s scheme. Let $l_p$ be the length of $p'$ and $q'$, let $l_h$ be the length of hash; the signature length in our scheme is about $9l_p+2l_h$; however, their signature length is at least $22l_p+8l_h$.

Through comparison of our scheme and Ateniese *et al*.'s scheme, we conclude that ours reduced computational cost and signature size.

## CONCLUSION

In this paper, we have proposed a novel group signature scheme with the security property of unforgeability, anonymity, unlinkability, untraceability, coalition-resistance, and the advantages that the group public key is constant, the signature size is independent of the number of group members. The total computation cost of signature and verification requires only 8 modular exponentiations.

## 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.

Joye, M., Lee, N.Y., Hwang, T., 1999a. On the Security of the Lee-Chang Group Signature Scheme and Its Derivatives. Information Security (ISW'99), LNCS 1729, Springer-Verlag, Berlin, p.47-51.

Joye, M., Kim, S., Lee, N.Y., 1999b. Cryptanalysis of Two Group Signature Schemes. Information Security (ISW'99), LNCS 1729, Springer-Verlag, Berlin, p.271-275.

Kim, S.J., Park, S.J., Won, D.H., 1996. Convertible Group Signatures. Asiacrypt'96, LNCS 1163, Springer-Verlag, Berlin, p.311-321.

Li, Z., Wang, Y., Yang, Y.X., Wu, W., 1999. Cryptanalysis of convertible group signature. *Electronics Letters*, **35**(5):1071-1072.

Park, S., Kim, S., Won, D., 1997. ID-based group signature. *Electronics Letters*, **33**(15):1616-1617.

Popescu, C., 2000. A modification of the Tseng-Jan group signature scheme. *Studia Univ. Babes-Bolyai, Informatica*, **XLV**(2):36-40.

Popescu, C., 2002. An efficient ID-based group signature scheme. *Studia Univ. Babes-Bolyai, Informatica*,

**XLVII**(2):29-36.

Saeednia, S., 2000. On the security of a convertible group signature schemes. *Information Processing Letters*, **73**:93-96.

Song, D.X., 2001. Practical Forward Secure Group Signature Schemes. Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS2001), Philadelphia, PA, USA, p.225-234.

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

Tseng, Y.M., Jan, J.K., 1998. A Novel ID-based Group Signature. *In*: Hwang, T.L., Lenstra, A.K.(Eds.), 1998 International Computer Symposium, Workshop on Cryptology and Information Security, Tainan, p.159-164.

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

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

Tseng, Y.M., Jan, J.K., 1999c. A Group Signature Scheme Using Self-certified Public Keys. Ninth National Conference on Information Security, p.165-172.

Wang, G.L., 2003a. Security Analysis of Several Group Signature Schemes. Indocrypt'2003, LNCS2904, Springer-Verlag, Berlin, p.252-265.

Wang, G.L., 2003b. On the Security of the Li-Hwang-Lee-Tsai Threshold Group Signature Scheme. Information Security and Cryptography (ICISC 2002), LNCS 2587, Springer-Verlag, Berlin, p.75-89.

Wang, G.L., 2004. On the Security of A Group Signature Scheme with Forward Security. Information Security and Cryptography (ICISC 2003), LNCS 2971, Springer-Verlag, Berlin, p.27-39.

Wang, C.H., Hwang, T., Lee, N.Y., 1999. Comments on two group signatures. *Information Processing Letters*, **69**:95-97.

Xia, S., You, J., 2002. A group signature scheme with strong separability. *The Journal of Systems and Software*, **60**(3):177-182.

Zhang, J., Wu, Q., Wang, Y., 2003. A Novel Efficient Group Signature Scheme with Forward Security. Information and Communications Security (ICICS'03), LNCS2836, Springer-Verlag, Berlin, p.292-300.