On the Security of a Group Signature Scheme with Strong Separability

LiHua Liu[†] Zhengjun Cao[‡]

[†]Department of Mathematics, ShangHai JiaoTong University. Shanghai, P.R. China.

[‡]Institute of System Science, Chinese Academy of Sciences. Beijing, P.R. China. *

Abstract A group signature scheme allows a group member of a given group to sign messages on behalf of the group in an anonymous and unlinkable fashion. In case of a dispute, however, a designated group manager can reveal the signer of a valid group signature. Many applications of group signatures require that the group manager can be split into a membership manager and a revocation manager. Such a group signature scheme with strong separability was proposed in paper [1]. Unfortunately, the scheme is insecure which has been shown in [2][3][4]. In this paper we show that the scheme is untraceable by a simple and direct attack. Besides, we show its universal forgeability by a general attack which only needs to choose five random numbers. We minutely explain the technique to shun the challenge in the scheme.

Keywords Group signature, Untraceability, Universal forgeability.

1 Introduction

Group signatures, introduced by Chaum and Heyst[5], allow individual members to make signatures on behalf of the group. More formally, a secure group signature scheme must satisfy the following properties[6]:

1. Unforgeability: Only group members are able to sign messages on behalf of the group.
2. Anonymity: Given a valid signature of some message, identifying the actual signer is computationally hard for everyone but the group manager.
3. Unlinkability: Deciding whether two different valid signatures were produced by the same group member is computationally hard.
4. Exculpability: Neither a group member nor the group manager can sign on behalf of other group member.

*‡Corresponding author's address: Institute of System Science, Chinese Academy of Sciences, Beijing, P.R. China. postcode: 100080. Tel: +86-010-82682282 E-mail: zjcamss@hotmail.com

5. Traceability: The group manager is always able to open a valid signature and identify of the actual signer.

6. Coalition-resistance: A colluding subset of 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.

Many applications of group signatures, for example, electronic market, require that the group manager can be split into a membership manager and a revocation manager. Such a group signature scheme with strong separability was proposed in paper [1]. Unfortunately, the scheme is insecure which has been shown in [2][3][4]. It has been shown that an adversary can make an universal forgery attack in paper [2]. Individual attack or coalition attack in order to produce a valid membership certification by legal group members has been presented in [3]. Paper [4] has shown that the scheme is linkable and universally forgeable. In this paper we show that the scheme is untraceable by a simple and direct attack. Besides, we show its universal forgeability by a general attack which only needs to choose five random numbers. We minutely explain the technique to shun the challenge in the scheme.

The rest of the paper is organized as follows. Section 2 first review the scheme proposed in [1]. We then analyze the scheme in Section 3 and 4, and explain the technique to shun the challenge in the scheme in section 5. Finally, some concluding remarks are given in Section 6.

2 Review of the scheme

The group signature scheme with strong separability consists of four kinds of participants, a trusted authority for generating secrets keys of all signers, a group manager for managing the memberships and identifying the signers, several signers (group members) for issuing group signatures and several verifiers for checking them. The group manager can also be split into a membership manager (for managing the memberships) and a revocation manager (for identifying the signers). Generally, the trusted authority can be appointed by the government. The scheme can be described as follows (refer to [1] for details):

2.1 Setup of trusted authority

The trusted authority generates two prime numbers p_1 and p_2. Let $m = p_1 p_2$ such that the Jacobi symbol $(2/m)$ is equal to -1. Subsequently, the authority publishes m and g but it keeps secret the prime factors p_1 and p_2.

2.2 Generating private keys

The trusted authority computes

$$ID_i = \begin{cases} D_i & if(D_i/m) = 1, \\ 2D_i & if(D_i/m) = -1. \end{cases}$$

where D_i is the identity information of signer U_i. In the case, the Jacobi symbol (ID_i/m) will be sure to equal to 1. Now the trusted authority computes the private key x_i for U_i such that

$$ID_i \equiv g^{x_i} \mod m$$

Then authority sends x_i to U_i in a secure way and U_i can check the validity of x_i by verifying the above equation.

2.3 Setup of group manager

The group manager chooses two large primes p_3 and p_4 such that $m < n = p_3 p_4$, and let e be an integer satisfying $gcd(e, \phi(n)) = 1$. Next, the group manager chooses two integers $x \in Z_m^*, h \in Z_m^*$, and computes $y = h^x \mod m$ satisfying $y \in Z_m^*$. Let H be a collision-resistant hash function. The public key of the group manager is (n, e, h, y, H) and his secret key is (x, d, p_3, p_4), where d satisfies $de \equiv 1 \mod \phi(n)$.

2.4 Generating membership keys

When a signer U_i wants to join the group, the group manager computes ID_i and

$$z_i = ID_i^d \mod n.$$

Then he sent z_i to U_i in secure way and U_i checks the validity of z_i by verifying

$$ID_i = z_i^e \mod n.$$

2.5 Signing phase

To sign a message M, U_i first chooses five random integers $\alpha, \beta, \theta, \omega \in Z_m$ and $\delta \in Z_n$. Then U_i computes

$$A = y^\alpha z_i \mod n, \quad B = y^\omega ID_i, \quad C = h^\omega \mod m.$$
$$D = H(y \parallel g \parallel h \parallel A \parallel B \parallel \hat{B} \parallel C \parallel v \parallel t_1 \parallel t_2 \parallel t_3 \parallel M)$$

where

$$\hat{B} = B \mod m, \qquad v = (A^e/B) \mod n,$$
$$t_1 = y^\delta \mod n, \qquad t_2 = y^\beta g^\theta \mod m, \quad t_3 = h^\beta \mod m.$$

$$E = \delta - D\varepsilon, \qquad \text{where} \quad \varepsilon = \alpha e - \omega,$$

and

$$F = \beta - D\omega, \qquad G = \theta - Dx_i.$$

Then U_i sends the signature (A, B, C, D, E, F, G) to the verifier.

2.6 Verification phase

Upon receiving the message M and signature (A, B, C, D, E, F, G), the verifier computes
$\hat{B}' = B \ mod \ m, \quad v' = A^e / B \ mod \ n,$
$t_1' = v'^D y^E \ mod \ n, \ \ t_2' = B'^D y^F g^G \ mod \ m, \ \ t_3' = C^D h^F \ mod \ m,$
$D' = H(y \parallel g \parallel h \parallel A \parallel B \parallel \hat{B}' \parallel C \parallel v' \parallel t_1' \parallel t_2' \parallel t_3' \parallel M).$

The verifier accepts the signature if and only if $D = D'$.

The correctness can be easily verified as follows:
$t_1' = v'^D y^E = y^{\varepsilon D} y^{\delta - D\varepsilon} = y^\delta = t_1 \ (mod \ n)$
$t_2' = B'^D y^F g^G = y^{\omega D} g^{x_i D} y^{\beta - D\omega} g^{\theta - D x_i} = y^\beta g^\theta = t_2 \ (mod \ m)$
$t_3' = C^D h^F = h^{\omega D} h^{\beta - D\omega} = h^\beta = t_3 \ (mod \ m)$

2.7 Opening signatures

The group manager recovers ID_i by computing

$$ID_i = B / C^x \ mod \ m.$$

3 Untraceability

Though the authors claimed that *the security of the scheme is based on the difficulty of the discrete logarithm problem (Camenisch, 1998) and on the security of Schnorr (1991) signature scheme, the RSA signature scheme, ElGamal encryption scheme,* we find it is not true. In the following we show that the scheme is untraceable by a simple and direct attack.

A group member U_i can generate a valid group signature which cannot be traced. He only needs to choose six random integers $\underline{\lambda}, \alpha, \beta, \theta, \omega \in Z_m$ and $\delta \in Z_n$. Then he computes

$$\bar{A} = \underline{g^\lambda} y^\alpha z_i \ mod \ n, \quad \bar{B} = \underline{g^{\lambda e}} y^\omega ID_i, \quad C = h^\omega \ mod \ m.$$

$$D = H(y \parallel g \parallel h \parallel \bar{A} \parallel \bar{B} \parallel \hat{\bar{B}} \parallel C \parallel v \parallel t_1 \parallel t_2 \parallel t_3 \parallel M)$$

where

$$\hat{\bar{B}} = \bar{B} \ mod \ m, \qquad v = (\bar{A}^e / \bar{B}) \ mod \ n,$$
$$t_1 = y^\delta \ mod \ n, \qquad t_2 = y^\beta g^\theta \ mod \ m, t_3 = h^\beta \ mod \ m.$$

and

$$E = \delta - D\varepsilon, \quad \text{where} \ \ \varepsilon = \alpha e - \omega,$$
$$F = \beta - D\omega, \quad \bar{G} = \theta - D x_i \underline{- \lambda e D}.$$

Then U_i sends the signature $(\bar{A}, \bar{B}, C, D, E, F, \bar{G})$ to the verifier.

Upon receiving the message M and signature $(\bar{A}, \bar{B}, C, D, E, F, \bar{G})$, the verifier computes

$$\hat{\bar{B}}' = \bar{B} \ mod \ m, \qquad v' = \bar{A}^e/\bar{B} \ mod \ n,$$
$$t_1' = v'^D y^E \ mod \ n, \qquad t_2' = \bar{B}'^D y^F g^{\bar{G}} \ mod \ m, \quad t_3' = C^D h^F \ mod \ m.$$

$$D' = H(y \parallel g \parallel h \parallel \bar{A} \parallel \bar{B} \parallel \hat{\bar{B}}' \parallel C \parallel v' \parallel t_1' \parallel t_2' \parallel t_3' \parallel M).$$

Comparing with original vision, we have

$$v' = \bar{A}^e/\bar{B} = \underline{g^{\lambda e}} A^e/(\underline{g^{\lambda e}} B) = A^e/B = y^{\varepsilon}, t_1' = t_1,$$

it only needs to verify:

$$\begin{aligned} t_2' &= \bar{B}'^D y^E g^{\bar{G}} \\ &= g^{\underline{\lambda eD}} y^{\omega D} g^{x_i D} y^{\beta - D\omega} g^{\theta - Dx_i - \underline{\lambda eD}} \\ &= y^{\beta} g^{\theta} = t_2 \ (mod \ m) \end{aligned}$$

Therefore, member U_i can forge valid signatures which are untraceable. In fact,

$$ID_i \neq \bar{B}/C^x \ mod \ m.$$

Remark: Underlined parts show the differentia between the attack and original scheme.

4 Universal forgeability

Wang has presented an attack on the scheme in [4], which shew that the scheme is universally forgeable. But Adversary has to select six random numbers in his attack. Now we show a new attack which only needs to choose five random numbers. It also shows that the scheme is universally forgeable.

Given a message M, to forge a signature, the adversary chooses five random numbers $\alpha, \beta, \theta, \delta, \omega$, computes

$$A = y^{\alpha}, \quad B = y^{\omega}, \quad C = h^{\omega}$$
$$t_1 = y^{\delta}, \quad t_2 = y^{\beta} g^{\theta}, \quad t_3 = h^{\beta}$$
$$v = A^e/B, \qquad \hat{B} = B \ (mod \ m)$$
$$D = H(y \parallel g \parallel h \parallel A \parallel B \parallel \hat{B} \parallel C \parallel v \parallel t_1 \parallel t_2 \parallel t_3 \parallel M)$$
$$E = \delta - eD\alpha + \omega D, \quad F = \beta - \omega D, \quad G = \theta.$$

Then he obtain a valid signature (A, B, C, D, E, F, G).

Correctness:

$$\begin{aligned} t'_1 &= v'^D y^E \\ &= A^{eD} B^{-D} y^E = y^{eD\alpha} y^{-\omega D} y^{\delta - eD\alpha + \omega D} \\ &= y^\delta = t_1 \ (mod\ n), \\ t'_2 &= B'^D y^F g^G \\ &= y^{\omega D} y^{\beta - \omega D} g^\theta = y^\beta g^\theta = t_2 \ (mod\ m), \\ t'_3 &= C^D h^F \\ &= h^{\omega D} h^{\beta - \omega D} = h^\beta = t_3 \ (mod\ m). \end{aligned}$$

Remark: Recently, we found that our above attack is just like that presented in [2]. But to explain our general technique to shun the challenge (see next section), we have to relate it here.

5 How to shun the challenge

In the section, we explain our general technique to shun the challenge in the scheme. It's helpful for those who want to design new secure group signature schemes in future.

First, from the form of $t'_3 = C^D h^F$, we know the challenge value D has to be counteracted in the expression. Therefore, we set

$$C := h^\omega \qquad \text{where } \omega \text{ is a random number.}$$

Hence, $t'_3 = h^{\omega D + F}$. Set

$$\beta := F + \omega D$$

we have $\boxed{t'_3 = h^\beta}$

Second, from the form of $t'_2 = B'^D y^F g^G = B'^D y^{\beta - \omega D} g^G$, we can assume $B' = y^{z_1}$ where z_1 is undetermined. Hence, we have

$$t'_2 = y^{z_1 D + \beta - \omega D} g^G$$

Therefore, set $z_1 = \omega$, we obtain $\boxed{t'_2 = y^\beta g^G}$

Finally, from the form of $t'_1 = v'^D y^E = A^{eD} B^{-D} y^E = A^{eD} y^{-\omega D + E}$, we can assume $A = y^\alpha$ where α is a random number. Hence, we have

$$t'_1 = y^{eD\alpha - \omega D + E}$$

Set

$$\delta := eD\alpha - \omega D + E$$

we have $\boxed{t'_1 = y^\delta}$

Therefore, we successfully shun the challenge in the scheme. It shows the scheme is universally forgeable.

6 Conclusion

In this paper, we presented a simple and direct attack on Xia-You group signature scheme. Our results show that their scheme is untraceable. Besides, we show its universal forgeability by a general technique to shun the challenge in the scheme. It's helpful for those who want to design new group signature schemes.

References

[1] Shundong Xia, Jinyuan You. A group signature scheme with strong separability. The Journal of Systems and Software 60 (2002) 177-182.

[2] Fangguo Zhang, Kwangjo Kim. Cryptanalysis of two signature schemes. Http:// eprint.iacr.org/2002/167.

[3] Zhang Jianhong, Wang Ji-lin, Wang YUmin. Two attacks on Xia-You group signature. Http:// eprint.iacr.org/2002/177.

[4] Guilin Wang. Security analysis of several group signature schemes. Http:// eprint.iacr.org/2003/194.

[5] D. Chaum and E. van Heyst. Group signatures. In: Advances in Cryptology-EUROCRYPT'91, LNCS 950, 257-265. Springer-Verlag, 1992.

[6] G. Ateniese, J.Camenisch, M.Joye, and G.Tsudik. A practical and provably secure coalition-resistant group signature scheme. In: Advances in Cryptology-CRYPTO'2000, LNCS 1880, 255-270. Springer-Verlag, 2000.