Analysis of One Popular Group Signature Scheme

Zhengjun Cao[1,2]

[1] Department of Mathematics, Shanghai University, Shanghai, China. 200444.
zjcamss@163.com
[2] Key Lab of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China.

Abstract. The group signature scheme [1], ACJT for short, is popular. In this paper we show that it is not secure. It does not satisfy exculpability. The group manager can sign on behalf of any group member. The drawback found in the scheme shows that some inductions are not sound, though they are prevalent in some so-called security proofs.
Keywords. group signature, exculpability, anonymity.

1 Introduction

Group signatures, introduced by Chaum and Heyst [2], allow individual members to make signatures on behalf of the group. Generally, a group signature must satisfy the following properties [1]:

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.
Traceability: The group manager is always able to open a valid signature and identify the actual signer.
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.
Exculpability: Neither a group member nor the group manager can sign on behalf of other group member.

Group signatures can be used to constitute a very useful primitive in many settings. It has become a hot problem to research group signatures in recent [3–7].

At Crypto'2000, Ateniese et al. [1] proposed a group signature scheme. The authors claimed that the scheme was practical and provably secure coalition-resistant. Recently, we find it is false. The group manager can sign on behalf of any group member. That is to say, the popular group signature scheme does not satisfy exculpability. It's the first time to show that the signature scheme is not secure. The attack developed in the paper is novel and interesting. The drawback found in the popular signature scheme shows that some inductions are not sound, though they are prevalent in so-called security proofs.

The rest of the paper is organized as follows. The next section reviews ACJT group signature scheme. An attack is presented in Section 3. Some conclusion remarks are given in Section 4.

2 Review

Let $\epsilon > 1, k, \ell_p$ be security parameters and let $\lambda_1, \lambda_2, \gamma_1, \gamma_2$ denote the lengths satisfying

$$\lambda_1 > \epsilon(\lambda_2 + k) + 2, \quad \lambda_2 > 4\ell_p, \quad \gamma_1 > \epsilon(\gamma_2 + k) + 2, \quad \gamma_2 > \lambda_1 + 2.$$

Define the integral ranges

$$\Lambda =]\, 2^{\lambda_1} - 2^{\lambda_2}, \;\; 2^{\lambda_1} + 2^{\lambda_2} \,[\,, \quad \Gamma =]\, 2^{\gamma_1} - 2^{\gamma_2}, \;\; 2^{\gamma_1} + 2^{\gamma_2} \,[.$$

Finally, let $\mathcal{H}$ be a collision-resistant hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^k$.

The initial phase involves the group manager (GM) setting the group public key $\mathcal{Y}$ and his secret key $\mathcal{S}$.

SETUP:

1. Select random secret ℓ_p–bit primes p', q' such that $p = 2p' + 1$ and $q = 2q' + 1$ are primes. Set the modulus $n = pq$.
2. Choose random elements $a, a_0, g, h \in_R QR(n)$ (of order $p'q'$).
3. Choose a random secret element $x \in_R Z^*_{p'q'}$ and set $y = g^x \bmod n$.
4. The group public key is : $\mathcal{Y} = (n, a, a_0, y, g, h)$.
5. The corresponding secret key (known only to GM) is: $\mathcal{S} = (p', q', x)$.

Suppose now that a new user wants to join the group. We assume that communication between the user and the group manager is secure. The selection of per-user parameters is done as follows:

JOIN:

1. User P_i generates a secret exponent $\bar{x}_i \in_R]0, 2^{\lambda_2}[$, a random integer $\bar{r} \in_R]0, n^2[$ and sends $C_1 = g^{\bar{x}_i} h^{\bar{r}} \mod n$ to GM and proves him knowledge of the representation of C_1 w.r.t. bases g and h.

2. GM checks that $C_1 \in QR(n)$. If this is the case, GM selects α_i and $\beta_i \in_R]0, 2^{\lambda_2}[$ at random and sends (α_i, β_i) to P_i.

3. User P_i computes $x_i = 2^{\lambda_1} + (\alpha_i \bar{x}_i + \beta_i \bmod 2^{\lambda_2})$ and sends GM the value $C_2 = a^{x_i} \bmod n$. The user also proves to GM:

   (a) that the discrete log of C_2 w.r.t. base a lies in Λ, and

(b) knowledge of integers u, v, and ω such that
i. u lies in $]-2^{\lambda_2}, 2^{\lambda_2}[$,
ii. u equals the discrete log of $C_2/a^{2^{\lambda_1}}$ w.r.t. base a, and
iii. $C_1^{\alpha_i} g^{\beta_i}$ equals $g^u (g^{2^{\lambda_2}})^v h^\omega$.

(The statements (i–iii) prove that the user's membership secret $x_i = \log_a C_2$ is correctly computed from C_1, α_i, and β_i.)

4. GM checks that $C_2 \in QR(n)$. If this is the case and all the above proofs were correct, GM selects a random prime $e_i \in_R \Gamma$ and computes $A_i := (C_2 a_0)^{1/e_i} \bmod n$. Finally, GM sends P_i the new membership certificate $[A_i, e_i]$. (Note that $A_i = (a^{x_i} a_0)^{1/e_i} \bmod n$.)

5. User P_i verifies that $a^{x_i} a_0 \equiv A_i^{e_i} \bmod n$.

Armed with a membership certificate $[A_i, e_i]$, a group member can generate anonymous and unlinkable group signatures on a generic message $m \in \{0,1\}^*$:

SIGN:

1. Generate a random value $\omega \in_R \{0,1\}^{2\ell_p}$ and compute:

$$T_1 = A_i y^\omega \bmod n, \quad T_2 = g^\omega \bmod n, \quad T_3 = g^{e_i} h^\omega \bmod n.$$

2. Randomly choose $r_1 \in_R \pm\{0,1\}^{\epsilon(\gamma_2+k)}$, $r_2 \in_R \pm\{0,1\}^{\epsilon(\lambda_2+k)}$, $r_3 \in_R \pm\{0,1\}^{\epsilon(\gamma_1+2\ell_p+k+1)}$, $r_4 \in_R \pm\{0,1\}^{\epsilon(2\ell_p+k)}$ and compute:

$$d_1 = T_1^{r_1}/(a^{r_2} y^{r_3}) \bmod n, \qquad d_2 = T_2^{r_1}/g^{r_3} \bmod n$$

$$d_3 = g^{r_4} \bmod n, \qquad d_4 = g^{r_1} h^{r_4} \bmod n$$

$$c = \mathcal{H}(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel d_1 \parallel d_2 \parallel d_3 \parallel d_4 \parallel m)$$

$$s_1 = r_1 - c(e_i - 2^{\gamma_1}), \qquad s_2 = r_2 - c(x_i - 2^{\lambda_1}),$$

$$s_3 = r_3 - c\, e_i\, \omega, \qquad s_4 = r_4 - c\,\omega \quad (\text{all in } \mathbf{Z}).$$

3. Output $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$.

A verifier can check the validity of a signature $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$ on the message m as follows:

VERIFY:

1. Compute

$$c' = \mathcal{H}(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel d_1' \parallel d_2' \parallel d_3' \parallel d_4' \parallel m)$$

where

$$d_1' = a_0^c T_1^{s_1 - c\,2^{\gamma_1}}/(a^{s_2 - c\,2^{\lambda_1}} y^{s_3}) \bmod n, \qquad d_2' = T_2^{s_1 - c\,2^{\gamma_1}}/g^{s_3} \bmod n,$$

$$d_3' = T_2^c g^{s_4} \bmod n, \qquad d_4' = T_3^c g^{s_1 - c\,2^{\gamma_1}} h^{s_4} \bmod n$$

2. Accept the signature if and only if $c = c'$ and

$$s_1 \in \pm\{0,1\}^{\epsilon(\gamma_2+k)+1}, \qquad s_2 \in \pm\{0,1\}^{\epsilon(\lambda_2+k)+1},$$

$$\underline{s_3 \in \pm\{0,1\}^{\epsilon(\gamma_1+2\ell_p+k+1)+1}}, \quad s_4 \in \pm\{0,1\}^{\epsilon(2\ell_p+k)+1}.$$

In case of a dispute, GM executes the following procedure:

OPEN:
1. Check the signature's validity via the VERIFY procedure.
2. Recover A_i (and thus the identity of P_i) as $A_i = T_1/T_2^x \bmod n$.
3. Prove that $\log_g y = \log_{T_2}(T_1/A_i \bmod n)$.

Remark 1: In the original description [1], we observe that

$$r_3 \in_R \pm\{0,1\}^{\epsilon(\gamma_1+2\ell_p+k+1)}, \quad s_3 \in \pm\{0,1\}^{\epsilon(\lambda_1+2\ell_p+k+1)+1}$$

It's not difficult to find it should be corrected to keep the consistency between r_3 and s_3.

3 Analysis

In this section, we show that ACJT group signature scheme doesn't satisfy exculpability. More precisely, we find the group manager (GM) can sign on behalf of any member if GM replaces Step 2 in the original SETUP phase with following:

2. Choose random elements $a_0, g, h \in_R QR(n)$ (of order $p'q'$) and set $a = a_0^t \pmod n$, where $t \in_R \mathbf{Z}^*_{p'q'}$.

Then GM records (a^{x_i}, A_i, e_i) in the JOIN phase (pointing to the member P_i). **Note that no member can prevent GM from setting** $a = a_0^t \pmod n$.

Using (t, a^{x_i}, A_i, e_i) and the secret key (p', q'), GM can sign on behalf of the member P_i. Given a message m, GM proceeds as follows:

1. Choose $\omega \in_R \{0,1\}^{2\ell_p}$ and compute:

$$T_1 = A_i y^{\omega} \bmod n, \quad T_2 = g^{\omega} \bmod n, \quad T_3 = h^{\omega} \bmod n.$$

2. Choose $b_1, b_2 \in_R \mathbf{Z}_n, r_4 \in_R \pm\{0,1\}^{\epsilon(2\ell_p+k)}$ and compute

$$d_1 = (a^{x_i})^{b_1} y^{b_2}, \quad d_2 = g^{b_2}, \quad d_3 = g^{r_4}, \quad d_4 = g^{b_1 e_i} h^{r_4} \pmod n.$$

$$c = \mathcal{H}(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel d_1 \parallel d_2 \parallel d_3 \parallel d_4 \parallel m)$$

3. Choose $X \in_R \Lambda$ and compute

$$R_1 = (c + b_1)\, e_i, \quad R_2 = c\, X + t^{-1}(c + b_1), \quad R_3 = \omega R_1 - b_2 \pmod{\phi(n)}$$

4. Choose proper $\rho_1, \rho_2, \rho_3 \in \mathbf{Z}$ such that

$$r_1 = R_1 + \rho_1\phi(n) \in \pm\{0,1\}^{\epsilon(\gamma_2+k)}$$
$$r_2 = R_2 + \rho_2\phi(n) \in \pm\{0,1\}^{\epsilon(\lambda_2+k)}$$
$$r_3 = R_3 + \rho_3\phi(n) \in \pm\{0,1\}^{\epsilon(\gamma_1+2\ell_p+k+1)}$$

(Since $R_1, R_2, R_3 \in \mathbf{Z}_n$, $n = (2p'+1)(2q'+1)$, $|p'| = |q'| = \ell_p$, $\epsilon > 1$, $\gamma_1 > \epsilon(\gamma_2 + k) + 2$, $\gamma_2 > \lambda_1 + 2$, $\lambda_1 > \epsilon(\lambda_2 + k) + 2$ and $\lambda_2 > 4\ell_p$, it's easy to find $\rho_1, \rho_2, \rho_3 \in \mathbf{Z}$ satisfying the above restrictions.)

5. Compute

$$s_1 = r_1 - c\,(e_i - 2^{\gamma_1}), \quad s_2 = r_2 - c\,(X - 2^{\lambda_1}),$$

$$s_3 = r_3 - c\,e_i\,\omega, \quad s_4 = r_4 - c\,\omega \quad (\text{all in } \mathbf{Z}).$$

6. Output $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$.

Correctness: For convenience, denote by ξ_i the inverse of e_i modulo $\phi(n)$, i.e.,

$$e_i\,\xi_i = 1 \bmod \phi(n)$$

Hence, we have

$$\begin{aligned}
d_1' &= a_0^c T_1^{s_1 - c2^{\gamma_1}} / (a^{s_2 - c2^{\lambda_1}} y^{s_3}) = a_0^c (A_i y^\omega)^{r_1 - ce_i} / (a^{r_2 - cX} y^{r_3 - ce_i\omega}) \\
&= a_0^c \left((a^{x_i} a_0)^{\xi_i}\right)^{(r_1 - ce_i)} y^{\omega r_1 - r_3} / a^{r_2 - cX} \\
&= (a^{x_i})^{r_1\xi_i - c} a_0^{c + r_1\xi_i - c} y^{\omega r_1 - r_3} / a^{r_2 - cX} = (a^{x_i})^{r_1\xi_i - c} a_0^{r_1\xi_i} y^{\omega r_1 - r_3} / a_0^{t(r_2 - cX)} \\
&= (a^{x_i})^{r_1\xi_i - c} a_0^{r_1\xi_i - t(r_2 - cX)} y^{\omega r_1 - r_3} = (a^{x_i})^{R_1\xi_i - c} a_0^{R_1\xi_i - t(R_2 - cX)} y^{\omega R_1 - R_3} \\
&= (a^{x_i})^{b_1} a_0^{c + b_1 - t(c + b_1)t^{-1}} y^{b_2} = (a^{x_i})^{b_1} y^{b_2} = d_1 \qquad (\bmod\ n)
\end{aligned}$$

$$\begin{aligned}
d_2' &= T_2^{s_1 - c2^{\gamma_1}} / g^{s_3} = (g^\omega)^{r_1 - ce_i} / g^{r_3 - ce_i\omega} \\
&= g^{\omega r_1 - r_3} = g^{\omega R_1 - R_3} = g^{b_2} = d_2 \qquad (\bmod\ n)
\end{aligned}$$

$$d_3' = T_2^c g^{s_4} = (g^\omega)^c g^{r_4 - \omega c} = g^{r_4} = d_3 \qquad (\bmod\ n)$$

$$\begin{aligned}
d_4' &= T_3^c g^{s_1 - c2^{\gamma_1}} h^{s_4} = (h^\omega)^c g^{r_1 - ce_i} h^{r_4 - c\omega} \\
&= g^{R_1 - ce_i} h^{r_4} = g^{b_1 e_i} h^{r_4} = d_4 \qquad (\bmod\ n)
\end{aligned}$$

Thus $c' = c$. It's easy to check that

$$s_1 \in \pm\{0,1\}^{\epsilon(\gamma_2 + k) + 1}, \quad s_2 \in \pm\{0,1\}^{\epsilon(\lambda_2 + k) + 1},$$

$$s_3 \in \pm\{0,1\}^{\epsilon(\gamma_1 + 2\ell_p + k + 1) + 1}, \quad s_4 \in \pm\{0,1\}^{\epsilon(2\ell_p + k) + 1}.$$

Clearly, we also have

$$T_1 / T_2^x = A_i y^\omega / (g^\omega)^x = A_i \qquad \bmod n$$

Therefore, the scheme is not exculpable.

Remark 2: The authors [1] claimed that

> First note that due to Corollary 2, GM does not get any information about a user's secret x_i apart from a^{x_i}. Thus, the value x_i is computationally hidden from GM. Next note that T_1, T_2, and T_3 are an unconditionally binding commitments to A_i and e_i. One can show that, if the factorization of n would be publicly known, the interactive proof underlying the group signature scheme is a proof of knowledge of the discrete log of $A_i^{e_i}/a_0$ (provided that ℓ_p is larger than twice to output length of the hash function / size of the challenges). Hence, not even the group manager can sign on behalf of P_i because computing discrete logarithms is assumed to be infeasible.

But by the above attack, GM is not forced to know a user's secret x_i even that T_1, T_2, and T_3 are an unconditionally binding commitments to A_i and e_i. We should stress that the likes of the above induction are not sound, though they are prevalent in some so-called security proofs.

4 Conclusion

In this paper we show that ACJT group signature scheme is insecure. The attack introduced in the paper will be helpful for researching group signature schemes in the future. Incidently, the fair E-cash system [8] directly based on ACJT fails. But it seems that the attack does not apply to the extensions of ACJT proposed in [9]. The extension proposed in [10] appears to resist the attack at the cost of the presence of a trusted third party.

Acknowledgements

I would like to express my sincere gratitude to my supervisor Professor M.L. Liu for many enlightening suggestions. Thanks also go to those anonymous referees who contributed with their expertise to the final version of the paper. This work is supported by National Natural Science Foundation of China (90304012) and Project 973 (2004CB318000).

References

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. *CRYPTO'2000*, LNCS 1880, pp.255–270. Springer-Verlag, 2000.
[2] D. Chaum and E. van Heyst. Group signatures. *EUROCRYPT'1991*, LNCS 547, pp.257–265. Springer-Verlag, 1992.
[3] D. Song. Practical forward-secure group signature schemes. *ACM Symposium on Computer and Communication Security*, pp.225–234, November 2001.
[4] E. Bresson and J. Stern. Efficient revocation in group signatures. *PKC'2001*, LNCS 1992, pp.190–206. Springer-Verlag, 2001.
[5] G. Ateniese and B. de Medeiros. Efficient group signatures without trapdoors. *ASIACRYPT'2003*, LNCS 2894, pp.246–268. Springer-Verlag, 2003.

[6] Mihir Bellare, Daniele Micciancio, Bogdan Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. *EUROCRYPT'2003*, LNCS 2656, pp.614–629. Springer-Verlag, 2003.

[7] D. Boneh, X. Boyen and H. Shacham. Short group signatures. *CRYPTO'2004*, LNCS 3152, pp.41–55. Springer-Verlag, 2004.

[8] Greg Maitland and Colin Boyd. Fair electronic cash based on a group signature scheme. *Information and Communications Security'2001*, LNCS 2229, pp.461–465. Springer-Verlag, 2001.

[9] J. Camenisch and J. Groth. Group Signatures: Better Efficiency and New Theoretical Aspects: *Forth Conference on Security in Communication Networks-SCN'04*. LNCS 3352, pp.120–133. Springer-Verlag, 2005.

[10] G. Tsudik, S. Xu. Accumulating composites and improved group signing. *ASIACRYPT 2003*, LNCS 2894, pp.269–286. Springer-Verlag, 2003.