Cryptanalysis of Qiu-Gu-Chen Variant Group Signature Scheme

Zhengjun Cao

Key Lab of Mathematics Mechanization, Academy of Mathematics and Systems Science,

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

(Graduate School of Chinese Academy of Sciences)

Abstract Qiu et al. proposed a variant group signature scheme in [1]. We find that the group manager can successfully forge signature because he has absolute predominance in Join Phase.

Keywords group signature scheme, forgeability.

1 Introduction

Group signatures, introduced by Chaum and Heyst[2], allow individual members to make signatures on behalf of the group. A secure group signature scheme must satisfy the following properties[3]: unforgeability, anonymity, unlinkability, exculpability, traceability, coalition-resistance. For more details, one can refer to [3].

In 2000, Qiu et al. proposed a **variant** group signature scheme in [1]. Here we omit the background and requirements of the model. We care naught for them, instead we care for its forgeability. We show that the group manager can successfully forge signature because he has absolute predominance in Join Phase.

2 Review of Qiu-Gu-Chen variant group signature scheme

The variant group signature consists of three entities: group manager (GM), group member, verifier.

Setup

GM randomly picks a RSA module n, two generators g, z of group Z_n^*, publishes (n, g, z).

Join

(1) A member U randomly picks two primes e, e' such that $\bar{e} = e \times e'$ is hard to factor.

(2) Compute $\bar{z} = z^{e'}\ mod\ n$.

(3) Pick $t_1, t_2 \in_R \{0,1\}^*$.

(4) Compute $\bar{c} = H(z \parallel \bar{z}^{t_1} \parallel z^{t_2} \parallel \bar{e})$, where $H(\cdot)$ is a public hash function.

(5) Compute $s_1 = t_1 - \bar{c}e, s_2 = t_2 - \bar{c}e'$, and send $(\bar{c}, s_1, s_2, \bar{z}, \bar{e})$ to GM.

(6) GM computes $y = z^{\bar{e}}, c' = H(z \parallel \bar{z}^{s_1}y^c \parallel z^{s_2}\bar{z}^c \parallel \bar{z} \parallel \bar{e})$, checks $\bar{c} = c'$. Otherwise, reject it.

(7) GM computes $u = \bar{z}^{\bar{d}}\ mod\ n$, where $\bar{d} \times \bar{e} = 1\ mod\ \varphi(n)$. GM sends u to the member U. Actually, $z^{e'} = \bar{z} = u^{\bar{e}} = u^{ee'}\ (mod\ n)$, hence, $z = u^e\ mod\ n$.

The member U keeps (u, e) in secret, sends $y\ (= g^e)$ to GM as his public key.

Sign

Given a message m, the member U signs it as follows:

(1) Pick $r \in_R \{0,1\}^*$, compute

$$d_1 = u^r, \qquad d_2 = g^r \ \ (mod\ n)$$

(2) Compute $c = H(g \parallel u \parallel z \parallel y \parallel d_1 \parallel d_2 \parallel m)$.

(3) Compute $s = r - ce$.

The signature of the message m is (c, s, u, y).

Verify

Given public parameters (n, g, z) and signature (m, c, s, u, y), Verifier checks

$$c \stackrel{?}{=} H(g \parallel u \parallel z \parallel y \parallel u^s z^c \parallel g^s y^c \parallel m)$$

If it holds, then Verifier accepts the signature. Otherwise, reject it.

3 Analysis

First, we should point out that the authors have claimed that the scheme was a variant group signature scheme, which did not satisfy some basic properties of a formal group signature scheme. In fact, it's obvious that the scheme does not satisfy full-anonymity[3] because the member U has to use his keys u, y to compound a signature (m, c, s, u, y). Why the authors called it variant group signature perplexes us.

Secondly, we find the scheme is forgeable. The group manager can successfully forge signatures because he has absolute predominance in Join Phase. A key observation is that the group public key is (n, g, z), GM can automatically generate valid key (u, e) for himself like any group member. In the following, we introduce another group manager's attack. It's more simple and direct.

Forgery procedure

Given a message m, GM only needs to:

(1) choose $\alpha, \lambda \in_R Z_n^*$

(2) compute

$$\beta = \lambda^{-1}\alpha \ \ mod\ \varphi(n), \qquad \tau = \lambda^{-1} \ \ mod\ \varphi(n)$$

(3) set

$$u = z^{\lambda} \ \ mod\ n, \qquad y = g^{\tau} \ \ mod\ n$$

(4) compute $c = H(g \parallel u \parallel z \parallel y \parallel z^{\alpha} \parallel g^{\beta} \parallel m)$

(5) compute $s = \beta - \tau c$

The signature of m is (c, s, u, y).

Correctness:

$$u^s z^c = (z^{\lambda})^s z^c = z^{\lambda s + c} = z^{\lambda(\beta - \tau c) + c} = z^{\lambda(\lambda^{-1}\alpha - \lambda^{-1}c) + c} = z^{\alpha}\ mod\ n$$

$$g^s y^c = g^{\beta - \tau c}(g^{\tau})^c = g^{\beta} \ \ mod\ n$$

4 Conclusion

In the paper, we analyze Qiu-Gu-Chen variant group signature scheme. Our results show that the scheme is insecure.

References

[1] Qiu Weidong, Gu Dawu, Chen Kefei. A new string-ring certificate hierarchy. ChinaCrypt'2000, pp.153-158.

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

[3] 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.