

TAMKANG UNIVERSITY
Department of Electrical Engineering
Laboratory of Cryptography and Information Security



Technical Report
TR-99-6B

**On the Difficulty of Coalition-Resistance
in Group Signature Schemes (II)**

Marc Joye

June 1, 1999

On the Difficulty of Coalition-Resistance in Group Signature Schemes (II)

Marc Joye*

June 1, 1999

Dept of Electrical Engineering, Tamkang University
Tamsui, Taipei Hsien, Taiwan 25137, R.O.C.
Email: joye@ug.ee.tku.edu.tw

Abstract. This report continues a discussion begun in the LCIS-98-17B report. As for the Ateniese-Tsudik schemes, we show that both the ID-based and self-certified public keys based group signature schemes proposed by Tseng and Jan (1998/1999) are not coalition-resistant: two colluding group members can produce untraceable group signatures.

Indexing terms: Digital signatures, Group signatures

1 Introduction

Most group signature schemes [1] are based on the discrete logarithm problem and are therefore not convenient to construct ID-based schemes [9]. A first attempt was made by Park, Kim, and Won [8]. However, their scheme was broken by Mao and Lim [6]: exploiting the prime order subgroup structure of the scheme, they showed that the anonymity of the signatures was not guaranteed. Moreover, the Park-Kim-Won scheme suffers from being rather expensive. The length of both the group public-key and the group signatures are proportional to the size of the group; more precisely, the identity of each group member must be included in the group public key, and if the group consists of k members a group signature requires k ordinary ElGamal-like signatures. Furthermore the scheme is ‘static’ in the sense that if new group members are added, the previously signed messages can no longer be verified with the updated public-key. A much better ID-based group signature scheme which does not present these limitations was recently proposed by Tseng and Jan [10]. Unfortunately, we will show that this signature is *not*

* Post-doctoral fellow of the National Science Council, Republic of China, under contract NSC88-2811-E-032-0001.

coalition-resistant. As in the Ateniese-Tsudik schemes [3], two colluding group members are able to produce valid group signatures which are untraceable by the group authority. In addition to their ID-based scheme, Tseng and Jan proposed a group signature scheme based on the related notion of self-certified public keys [2]. This latter, also, is subject to coalition attacks.

2 Tseng-Jan ID-based Group Signature

In this section, we give a short description of the Tseng-Jan group signature scheme and refer to the original paper [10] for more details. Next, we show how two colluding members are able to produce an untraceable (yet valid) signature.

2.1 Description

The scheme is divided into 5 algorithms: `setup`, `join`, `sign`, `verify` and `open`. In the `setup` algorithm, a trusted authority and the group authority select the parameters of the scheme; the `join` algorithm enables a new user to join the group; the `sign` algorithm is the signature algorithm; the `verify` algorithm allows to check the validity of a signature; and the `open` algorithm enables the group authority to ‘open’ a signature to reveal the identity of the signer in case of disputes.

To `setup` the system, a trusted authority selects two large primes $p_1 (\equiv 3 \pmod{8})$ and $p_2 (\equiv 7 \pmod{8})$ such that $(p_1 - 1)/2$ and $(p_2 - 1)/2$ are smooth, odd and relatively co-prime [7]. Let $N = p_1 p_2$. The trusted authority also defines e, d, v and t satisfying $ed \equiv 1 \pmod{\varphi(N)}$ and $vt \equiv 1 \pmod{\varphi(N)}$, selects g of large order in \mathbb{Z}_N^* , and computes $F = g^v \pmod{N}$. Moreover, the group authority chooses a secret key x and computes the corresponding public key $y = F^x \pmod{N}$. The public parameters are (N, e, g, F, y) ; the secret parameters are (p_1, p_2, d, v, t, x) . When a user U_i (with identity information D_i) wants to `join` the group, the trusted authority computes $s_i = et \log_g ID_i \pmod{\varphi(N)}$ where $ID_i = D_i$ or $2D_i$ according to $(D_i|N) = 1$ or -1 , and the group authority computes $x_i = ID_i^x \pmod{N}$. The user membership certificate is the pair (s_i, x_i) . To `sign` a message M , user U_i chooses two random numbers r_1 and r_2 and computes $A = y^{r_1} \pmod{N}$, $B = y^{r_2 e} \pmod{N}$, $C = s_i + r_1 h(M||A||B) + r_2 e$ and $D = x_i y^{r_2 h(M||A||B)} \pmod{N}$, where $h(\cdot)$ is a publicly known hash function. Then, to `verify` that (A, B, C, D) is a valid group signature for message M , one checks whether $D^e A^{h(M||A||B)} B \equiv y^C B^{h(M||A||B)} \pmod{N}$. In case of disputes, the group authority can `open` the signature to recover who issued it by checking which identity ID_i satisfies the relation $ID_i^{x_i} \equiv D^e B^{-h(M||A||B)} \pmod{N}$.

2.2 Coalition Attack

We now show how to produce a valid membership certificate without the help of the group authority.

Let indexes 1 and 2 respectively denote the attributes of user 1 and user 2. If the two users collude, then they can easily evaluate $y^d \bmod N$ as follows. Since $s_i = et \log_g ID_i \bmod \varphi(N)$, we have $g^{s_i} \equiv ID_i^{et} \pmod{N}$. Hence, from $x_i = ID_i^x \bmod N$, it follows that

$$x_i^e \equiv (ID_i^e)^x \equiv (g^{s_i t^{-1}})^x \equiv (g^{vx})^{s_i} \equiv y^{s_i} \pmod{N} .$$

So, $x_1 = (y^d)^{s_1} \bmod N$, and similarly $x_2 = (y^d)^{s_2} \bmod N$. Assuming w.l.o.g. that $\gcd(s_1, s_2) = 1$, users 1 and 2 can use the extended Euclidean algorithm to find $\alpha, \beta \in \mathbb{Z}$ such that $\alpha s_1 + \beta s_2 = 1$. Consequently, they can recover

$$y^d \equiv y^{d(\alpha s_1 + \beta s_2)} \equiv x_1^\alpha x_2^\beta \pmod{N}$$

from x_1 and x_2 .

Once $y^d \bmod N$ is known, a new membership certificate can be computed as (s', x') with $x' = (y^d)^{s'} \bmod N$ for an arbitrary s' . Noting that $x'^e \equiv y^{s'}$ \pmod{N} , the signatures produced with this certificate will be valid. However since this certificate does not correspond to a known identity, the group authority will not be able to open the resulting signatures.

Remark 1. In addition to be vulnerable against coalition attacks, the Tseng-Jan ID-based signature is *universally* forgeable [5], that is, everyone is able to forge a valid group signature for an arbitrary message M . There are two attacks on the scheme. In the first attack, an adversary randomly chooses C and D , computes $B = y^C D^{-e} \bmod N$, and sets $A = B$. One can easily see that (A, B, C, D) is a valid signature for any message M .

The second attack allows to choose $A \neq B$. The adversary chooses D and an integer ω . Then she computes $B = D^{-e} \bmod N$, $A = B y^\omega \bmod N$, and $C = \omega \cdot h(m \| A \| B)$ (over \mathbb{Z}). Here too, one easily verifies that (A, B, C, D) is a valid signature on message M .

3 Tseng-Jan Self-Certified Public-Keys based Group Signature

In this section, we show that the previously described attack still applies to the second scheme of Tseng and Jan [11]: two colluding members can easily derive a new (and valid) membership certificate.

3.1 Description

We begin with a brief review of the scheme and refer to [11] for a thorough description. The `setup` goes as follows: a trusted authority selects $N = pq$ with $p = 2p' + 1$ and $q = 2q' + 1$ where p, q, p' and q' are all prime; he also selects g of order $\nu = p'q'$ and $e, d \in \mathbb{Z}_\nu^*$ satisfying $ed \equiv 1 \pmod{\nu}$. The group authority (with

identity information GD) chooses a secret key x and computes $z = g^x \bmod N$. After receiving z , the trusted authority computes $y = (g^x)^{GID^{-1}} \bmod N$ where $GID = f(GD)$ for a publicly known hash function $f(\cdot)$, and the group secret key $s_G = (g^x)^{-d} \bmod N$. He sends s_G to the group authority. The public parameters are (N, e, g, y) ; the secret parameters are (p, q, d, x, s_G) . To join the group, a user U_i (with identity information D_i) chooses a secret key s_i , computes $z_i = g^{s_i} \bmod N$, and sends z_i to the trusted authority. The trusted authority then sends back $p_i = (g^{s_i})^{ID_i^{-1}d} \bmod N$ where $ID_i = f(D_i)$. From p_i , the group authority computes $x_i = p_i^{ID_i x} s_G \bmod N$. The membership certificate of user U_i is the pair (s_i, x_i) . When U_i wants to sign a message M , she chooses r_1, r_2 and r_3 at random and computes $A = r_1 s_i$, $B = r_2^{-eA} \bmod N$, $C = y^{GID A r_3} \bmod N$, $D = s_i h(M \| A \| B \| C) + r_3 C$ (where $h(\cdot)$ is a publicly known hash function), and $E = x_i r_2^{h(M \| A \| B \| C \| D)} \bmod N$. To verify the validity of signature (A, B, C, D, E) on message M , one checks whether $y^{GID A D} \equiv (E^{eA} B^{h(M \| A \| B \| C \| D)} y^{GID A})^{h(M \| A \| B \| C)} C^C \pmod{N}$. In case of disputes, the group authority can open the signature by checking which x_i satisfies the relation $(x_i)^{eA} B^{-h(M \| A \| B \| C \| D)} \equiv E^{eA} \pmod{N}$.

3.2 Coalition Attack

As before, let indexes 1 and 2 respectively denote the attributes of user 1 and user 2. If the two users collude then they can recover the group secret key $s_G = g^{-xd} \bmod N$. We assume w.l.o.g. that $\gcd(s_1 - 1, s_2 - 1) = 1$. So, by the extended Euclidean algorithm, there exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha(s_1 - 1) + \beta(s_2 - 1) = 1$. Moreover, we have $x_i = p_i^{ID_i x} s_G \equiv g^{-xd(-s_i+1)} \equiv s_G^{-s_i+1} \pmod{N}$. Hence, from their membership certificates (s_1, x_1) and (s_2, x_2) , users 1 and 2 can find

$$s_G \equiv s_G^{\alpha(s_1-1)+\beta(s_2-1)} \equiv x_1^{-\alpha} x_2^{-\beta} \pmod{N} .$$

Consequently, the second Tseng-Jan does not offer coalition-resistance: given s_G , users 1 and 2 can produce a new valid certificate of their choice as (s', x') where $x' = s_G^{-s'+1} \bmod N$ for some arbitrary s' .

Remark 2. We note that the previous scheme presents other weaknesses. For example, the tuple $(A, B = 1, C = 1, D = h(M \| A \| B \| C), E = 1)$ (for a random number A) is an universal signature on message M .

Remark 3. Kim [4] also notes that a single member can produce an untraceable signature. From her membership certificate (s_i, x_i) , the (malicious) member U_i can derive a new certificate $(s', x') = (s_i^2, x_i^{s_i+1} \bmod N)$, where s_i^2 is computed over \mathbb{Z} . One can see that this latter certificate is valid since $x' \equiv x_i^{s_i+1} \equiv (s_G^{-s_i+1})^{s_i+1} \equiv s_G^{-s'+1} \pmod{N}$.

Acknowledgements

The author is grateful to Narn-Yih Lee for pointing out that the Tseng-Jan ID-based signature is universally forgeable. Thanks also go to Seungjoo Kim for commenting that a single member is able to produce a untraceable signature in the second Tseng-Jan scheme.

References

- [1] David Chaum and Eugène van Heijst, *Group signatures*, Advances in Cryptology — EUROCRYPT '91 (D.W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 257–265.
- [2] Marc Girault, *Self-certified public keys*, Advances in Cryptology – EUROCRYPT '91 (D.W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 491–497.
- [3] Marc Joye, *On the difficulty of coalition-resistance in group signature schemes (I)*, Tech. Report 98-17B, LCIS Tamkang, Tamsui, November 1998.
- [4] Seungjoo Kim, *On Tseng-Jan self certified public-keys based group signature*, Unpublished manuscript, May 31, 1999.
- [5] Narn-Yih Lee, *Personal communication*, May 19, 1999.
- [6] Wenbo Mao and Chae Hoon Lim, *Cryptanalysis in prime order subgroups of \mathbb{Z}_n* , Advances in Cryptology — ASIACRYPT '98 (K. Ohta and D. Pei, eds.), Lecture Notes in Computer Science, vol. 1514, Springer-Verlag, 1998, pp. 214–226.
- [7] Ueli M. Maurer and Yacov Yacobi, *Non-interactive public-key cryptography*, Advances in Cryptology – EUROCRYPT '91 (D.W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 498–507.
- [8] Sangjoon Park, Seungjoo Kim, and Dongho Won, *ID-based group signature*, Electronics Letters **33** (1997), no. 19, 1616–1617.
- [9] Adi Shamir, *Identity-based cryptosystems and signatures schemes*, Advances in Cryptology – Proceedings of CRYPTO 84 (G.R. Blakley and D. Chaum, eds.), Lecture Notes in Computer Science, vol. 196, Springer-Verlag, 1985, pp. 47–53.
- [10] Yuh-Min Tseng and Jinn-Ke Jan, *A novel ID-based group signature*, 1998 International Computer Symposium, Workshop on Cryptology and Information Security (T.L. Hwang and A.K. Lenstra, eds.), Tainan, December 17–19, 1998, pp. 159–164.
- [11] ———, *A group signature scheme using self-certified public keys*, Ninth National Conference on Information Security, Taichung, May 14–15, 1999, pp. 165–172.