Cryptanalysis of Two Group Signature Schemes

[Published in M. Mambo and Y. Zheng, Eds., *Information Security*, vol. 1729 of *Lecture Notes in Computer Science*, pp. 271–275, Springer-Verlag, 1999.]

Marc Joye[1,⋆], Seungjoo Kim[2], and Narn-Yih Lee[3]

[1] Gemplus Card International
Parc d'Activités de Gémenos, B.P. 100, 13881 Gémenos, France
marc.joye@gemplus.com
[2] Korea Information Security Agency (KISA)
5th FL., Dong-A Tower, 1321-6, Seocho-Dong, Seocho-Gu, Seoul 137-070, Korea
skim@kisa.or.kr
[3] Dept of Applied Foreign Language, Nan-Tai Institute of Technology
Tainan, Taiwan 710, R.O.C.
nylee@mail.ntc.edu.tw

Abstract. Group signature schemes allow a group member to anonymously sign on group's behalf. Moreover, in case of anonymity misuse, a group authority can recover the issuer of a signature. This paper analyzes the security of two group signature schemes recently proposed by Tseng and Jan. We show that both schemes are universally forgeable, that is, anyone (not necessarily a group member) is able to produce a valid group signature on an arbitrary message, which cannot be traced by the group authority.

Keywords. Digital signatures, group signatures, cryptanalysis, universal forgeries.

1 Introduction

Group signature schemes [3] allow a group member to anonymously sign on group's behalf. Moreover, in case of anonymity misuse, a group authority can recover the issuer of a signature. These schemes are especially useful in (off-line) e-cash systems [5, 11] and electronic voting protocols [8] where they enable to protect user's privacy. The state-of-the-art is exemplified by the recent scheme of Camenisch and Michels [2].

Following the previous work of [9] (flawed in [6] and revised in [10]), Tseng and Jan propose an ID-based group signature scheme [12]. In [13], they also propose a group signature scheme based on the related notion of self-certified public keys [4]. In this paper, we show that their two schemes are universally

⋆ Part of this work was performed while the author was with the Dept of Electrical Engineering, Tamkang University, Tamsui, Taiwan 251, R.O.C.

forgeable, that is, anyone (not necessarily a group member) is able to produce a valid group signature on an arbitrary message, which cannot be traced by the group authority.

The rest of this paper is organized as follows. In Section 2, we review the two schemes proposed by Tseng and Jan. Next, in Section 3, we point out universal forgeries. Finally, we conclude in Section 4.

2 Tseng-Jan Group Signature Schemes

In this section, we give a short description of the two Tseng-Jan group signature schemes and refer to the original papers [12, 13] for more details.

Both schemes involve four parties: a trusted authority, the group authority, the group members, and verifiers. The *trusted authority* acts as a third helper to setup the system parameters. The *group authority* selects the group public/secret keys; he (jointly with the trusted authority) issues membership certificates to new users who wish to join the group; and, in case of disputes, opens the contentious group signatures to reveal the identity of the actual signer. Finally, *group members* anonymously sign on group's behalf using their membership certificates; and *verifiers* check the validity of the group signatures using the group public key.

2.1 ID-based signature

For setting up the system, a trusted authority selects two large primes p_1 ($\equiv 3 \bmod 8$) and p_2 ($\equiv 7 \bmod 8$) such that $(p_1 - 1)/2$ and $(p_2 - 1)/2$ are smooth, odd and co-prime [7]. Let $N = p_1\, p_2$. The trusted authority also defines e, d, v, 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 $F = g^v \bmod N$. Moreover, the group authority chooses a secret key x and computes the corresponding public key $y = F^x \bmod N$. 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

$$s_i = et \log_g ID_i \bmod \varphi(N) \tag{1}$$

where $ID_i = D_i$ or $2D_i$ according to $(D_i|N) = 1$ or -1, and the group authority computes

$$x_i = {ID_i}^x \bmod N \ . \tag{2}$$

The user membership certificate is the pair (s_i, x_i). To sign a message M, user U_i (with certificate (s_i, x_i)) chooses two random numbers r_1 and r_2 and computes $A = y^{r_1} \bmod N$, $B = y^{r_2\, e} \bmod N$, $C = s_i + r_1\, h(M\|A\|B) + r_2\, e$ and $D = x_i\, y^{r_2\, h(M\|A\|B)} \bmod N$, where $h(\cdot)$ is a publicly known hash function. The group signature on message M is given by the tuple (A, B, C, D). The validity of this signature can then be verified by checking whether

$$D^e\, A^{h(M\|A\|B)}\, B \equiv y^C\, B^{h(M\|A\|B)} \pmod N \ . \tag{3}$$

Finally, in case of disputes, the group authority can open the signature to recover who issued it by checking which identity ID_i satisfies ${ID_i}^{xe} \equiv D^e\, B^{-h(M\|A\|B)} \pmod N$.

2.2 Self-certified public keys based signature

In the second scheme, the setup goes as follows. A trusted authority selects $N = pq$ with $p = 2p' + 1$ and $q = 2q' + 1$ where p, q, p', 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 $y = z^{GID^{-1}} \bmod N$ where $GID = f(GD)$ for a publicly known hash function $f(\cdot)$, and the group secret key $s_G = z^{-d} \bmod N$. 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 $p_i = (z_i)^{ID_i^{-1}\, d} \bmod N$ where $ID_i = f(D_i)$. From p_i, the group authority computes

$$x_i = {p_i}^{ID_i\, x}\, s_G \bmod N \ . \tag{4}$$

The membership certificate of user U_i is the pair (s_i, x_i). When U_i wants to sign a message M, he 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

$$y^{GID\, A\, D} \equiv (E^{eA}\, B^{h(M\|A\|B\|C\|D)}\, y^{GID\, A})^{h(M\|A\|B\|C)}\, C^C \pmod N \ . \tag{5}$$

In case of disputes, the group authority opens 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 Cryptanalysis

3.1 On the security of the ID-based scheme

To become a group member, each new user is issued a membership certificate which is then used to generate group signatures. In the ID-based scheme, the membership certificate (see Eqs (1) and (2)) is given by the pair $(s_i, x_i) = (et \log_g ID_i \bmod \varphi(N), {ID_i}^x \bmod N)$. So, noting that $g^{s_i} \equiv {ID_i}^{et} \pmod N$, it follows that

$${x_i}^e \equiv ({ID_i}^e)^x \equiv (g^{s_i\, t^{-1}})^x \equiv (g^{vx})^{s_i} \equiv y^{s_i} \pmod N \ . \tag{6}$$

Hence, if $s_i = ke$ for some integer k, then we have $x_i \equiv y^k \pmod N$. This means that $(s_i, x_i) = (ke, y^k \bmod N)$ is a valid membership certificate for any

integer k. In particular, for $k = 0$, the pair $(s_i, x_i) = (0, 1)$ is a valid certificate. Therefore, an adversary can forge a Tseng-Jan ID-based group signature on an arbitrary message M as follows:

(1) Randomly choose r_1 and r_2;
(2) Compute $A = y^{r_1} \bmod N$, $B = y^{r_2\, e} \bmod N$, $C = r_1\, h(M\|A\|B) + r_2\, e$, and $D = y^{r_2\, h(M\|A\|B)} \bmod N$;
(3) The group signature is given by (A, B, C, D).

The above attack clearly exhibits that, contrary to what is claimed in [12], the security of the scheme does not rely on the discrete logarithm problem. Moreover, this attack can easily be generalized by considering the more general *representation problem* (see [1]) as follows. Let β be an element in $\mathbb{Z}_N^*$, and let $A = y^{a_1}\, \beta^{a_2} \bmod N$, $B = y^{b_1}\, \beta^{b_2} \bmod N$ and $D = y^{d_1}\, \beta^{d_2} \bmod N$ respectively denote the representations of A, B and D w.r.t. bases y and β. The verification equation (Eq. (3)) then becomes

$$(y^{d_1}\, \beta^{d_2})^e\, (y^{a_1}\, \beta^{a_2})^{h(M\|A\|B)}\, (y^{b_1}\, \beta^{b_2}) \equiv y^C\, (y^{b_1}\, \beta^{b_2})^{h(M\|A\|B)} \pmod N,$$

which is satisfied whenever

$$\begin{cases} d_1\, e + a_1\, h(M\|A\|B) + b_1 \equiv C + b_1\, h(M\|A\|B) \\ d_2\, e + a_2\, h(M\|A\|B) + b_2 \equiv b_2\, h(M\|A\|B) \end{cases} \pmod{\varphi(N)}\ . \qquad (7)$$

The first equation in (7) is trivially satisfied if $C = d_1 e + (a_1 - b_1)\, h(M\|A\|B) + b_1$, whereas the second equation is trivially satisfied if $a_2 = b_2 = -d_2\, e$ (over $\mathbb{Z}$). To sum up, an adversary can thus forge a Tseng-Jan ID-based group signature on an arbitrary message M as follows:

(1) Randomly choose β, a_1, b_1, d_1 and d_2, and set $a_2 = b_2 = -d_2\, e$ (over $\mathbb{Z}$);
(2) Compute $A = y^{a_1}\, \beta^{a_2} \bmod N$, $B = y^{b_1}\, \beta^{b_2} \bmod N$ and $D = y^{d_1}\, \beta^{d_2} \bmod N$;
(3) Compute $C = d_1 e + (a_1 - b_1)\, h(M\|A\|B) + b_1$;
(4) The group signature is given by (A, B, C, D).

Note that the first attack corresponds to the special case $d_2 = 0$.

3.2 On the security of the self-certified public keys based scheme

The self-certified public keys based scheme seems more robust. However, we will see that the previous attack still applies. From $p_i = (g^{s_i})^{ID_i^{-1} d} \bmod N$ and $s_G = (g^x)^{-d} \bmod N$, we have

$$x_i{}^e \equiv (p_i{}^{ID_i\, x}\, s_G)^e \equiv g^{s_i x}\, g^{-x} \equiv g^{x(s_i - 1)} \equiv y^{GID(s_i - 1)} \pmod N\ . \qquad (8)$$

Therefore, $(s_i, x_i) = (1 + ke, (y^{GID})^k \bmod N)$ is a valid membership certificate for any integer k. In particular, $(s_i, x_i) = (1, 1)$ is a valid certificate. As before, an adversary can thus forge a Tseng-Jan self-certified public keys based group signature on an arbitrary message M as follows:

(1) Randomly choose r_1, r_2, and r_3;

(2) Set $A = r_1$;
(3) Compute $B = {r_2}^{-eA} \bmod N$, $C = y^{GID\, A r_3} \bmod N$, $D = h(M\|A\|B\|C) + r_3\, C$, and $E = {r_2}^{h(M\|A\|B\|C\|D)} \bmod N$;
(4) The group signature is given by (A, B, C, D, E).

Here too, we see that the security of scheme does not rely on the representation problem (consider bases y and r_2) and a fortiori on the discrete logarithm problem. Furthermore, as before, the strategy can easily be generalized.

4 Conclusions

We have shown that the two group signature schemes proposed by Tseng and Jan are *universally* forgeable. This illustrates once more that ad-hoc constructions — although seemingly robust — certainly do not constitute a security proof and that their use always present some risks.

References

1. Stefan Brands, *An efficient off-line electronic cash system based on the representation problem*, Technical Report CS-R9323, Centrum voor Wiskunde en Informatica, April 1993.
2. Jan Camenisch and Markus Michels. A group signature scheme with improved efficiency. In *Advances in Cryptology – ASIACRYPT '98*, LNCS 1514, pp. 160–174. Springer-Verlag, 1998.
3. David Chaum and Eugène van Heijst. Group signatures. In *Advances in Cryptology – EUROCRYPT '91*, LNCS 547, pp. 257–265. Springer-Verlag, 1991.
4. Marc Girault. Self-certified public keys. In *Advances in Cryptology – EUROCRYPT '91*, LNCS 547, pp. 491–497. Springer-Verlag, 1991.
5. Anna Lysyanskaya and Zulfikar Ramzan. Group blind signatures: A scalable solution to electronic cash. In *Financial Cryptography (FC '98)*, LNCS 1465, pp. 184–197. Springer-Verlag, 1998.
6. Wenbo Mao and Chae Hoon Lim. Cryptanalysis in prime order subgroups of $\mathbb{Z}_n$. In *Advances in Cryptology – ASIACRYPT '98*, LNCS 1514, pp. 214–226. Springer-Verlag, 1998.
7. Ueli M. Maurer and Yacov Yacobi. Non-interactive public-key cryptography. In *Advances in Cryptology – EUROCRYPT '91*, LNCS 547, pp. 498–507. Springer-Verlag, 1991.
8. Toru Nakanishi, Toru Fujiwara and Hajime Watanabe. A secret voting protocol using a group signature scheme. Technical Report ISEC96-23, IEICE, September 1996.
9. Sangjoon Park, Seungjoo Kim and Dongho Won. ID-based group signature. *Electronics Letters*, 33(19):1616–1617, 1997.
10. Sangjoon Park, Seungjoo Kim and Dongho Won. On the security of ID-based group signature. *Journal of the Korean Institute of Information Security and Cryptology*, 8(3):27–37, 1998.
11. Jacques Traoré. Group signatures and their relevance to privacy-protecting offline electronic cash systems. In *Information Security and Privacy (ACISP '99)*, LNCS 1587, pp. 228–243. Springer-Verlag, 1999.

12. Yuh-Min Tseng and Jinn-Ke Jan. A novel ID-based group signature. In T. L. Hwang and A. K. Lenstra, editors, *1998 International Computer Symposium, Workshop on Cryptology and Information Security* (Tainan, December 17–19, 1998), pp. 159–164.
13. ———. A group signature scheme using self-certified public keys. In *Ninth National Conference on Information Security* (Taichung, May 14–15, 1999), pp. 165–172.