

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



Technical Report
TR-98-17B

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

Marc Joye

November 4, 1998

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

Marc Joye*

November 4, 1998

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

Abstract. Very recently, Ateniese and Tsudik suggested two nice and practical group signature schemes allowing members of a group to sign on behalf of the group in such a way that the signer's identity can be recovered by the group manager in case of abuse. Their first scheme does not address hostile coalition of group members while the second one is supposed to be coalition-resistant. This report shows that this additional property is not satisfied: two colluding group members can produce untraceable group signatures.

Indexing terms: Digital signatures, Group signatures

1 Group Signatures

Group signatures, introduced by Chaum and van Heijst [4], are digital signatures allowing members of a group to sign on behalf the group so that

- only group members can sign messages;
- the receiver of the signature can verify whether the signature is valid for the group, but cannot determine which member of the group made the signature;
- in the case of dispute, the signature can be opened to reveal the identity of the signer.

Such a signature scheme can for example be used in invitations to submit tenders [5]. All companies submitting a tender then form a group and each company signs its tender anonymously using the group signature. Later when the preferred

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

tender has been selected, the signer can be detected whereas the signers of all other tenders remain anonymous. Another application is the construction of electronic cash system in which several banks can securely distribute anonymous and untraceable e-cash. The group property presents then the further advantage to also conceal the identity of the issuing bank [6].

Two very nice realizations of group signature schemes were recently proposed by Ateniese and Tsudik [1, 2]. Their schemes present the advantages of being very efficient; in particular, the size of the group public key and the length of a group signature do not depend on the group size. However, two group members can pool their secrets together so that the resulting group signature is untraceable (albeit valid) by the group manager. This means that these signature schemes are restricted to some specialized applications such as electronic lotteries.

2 Coalition Attack

In this section, we briefly review the second group signature scheme of Ateniese and Tsudik. We refer to the original paper [2] for a more complete description. The scheme is divided into 5 algorithms: `setup`, `join`, `sign` and `verify` and `open`. We will mainly be concerned with the `join` algorithm which enables a new user to join the group and show how to produce a valid membership certificate without the help of the group manager.

It is useful to introduce some notations. The Schnorr proof of knowledge [7] the (secret) discrete logarithm y (with respect to base b) is the square of the (secret) discrete logarithm x (with respect to base a) will be denoted as $\text{SKSQ}(m, a^x, b^y, a, b)$. Moreover, unless otherwise specified, all the computations are supposed to be done in the ring \mathbb{Z}_n , where n is a safe RSA modulus.

2.1 Ateniese-Tsudik signature scheme II

Notations. The public parameters are n, v (prime), $a, b, Y_1 = a^{-y_1}, Y_2 = b^{-y_2}$ and $Z = a^z$; the secret parameters are y_1, y_2, z and the factors of n .

In the second scheme [2], the `join` procedure goes as follows. The user chooses a secret exponent ℓ_1 and sends a^{ℓ_1} to the group manager. The group manager then sends a random number ℓ_2 to the user. The user computes $x = \ell_1 \ell_2$ and sends $(a^x, \text{SKSQ}(\text{“join”}, a^x, b^{x^2}, a, b))$ and a proof that $0 < x < v$. The group manager then verifies the proof of knowledge of x , that $(a^{\ell_1})^{\ell_2} = a^x$ and the proof that $0 < x < v$. After these verifications, the group manager sends the membership certificate $(A = a^{(x+y_1)v^{-1}}, B = b^{(x^2+y_2)v^{-1}})$.

2.2 Colluding group members

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 $a^{v^{-1}}$ and $a^{y_1 v^{-1}}$ as follows. From $A_1 =$

$a^{(x_1+y_1)v^{-1}}$ and $A_2 = a^{(x_2+y_1)v^{-1}}$, they compute $M = A_1/A_2 = a^{(x_1-x_2)v^{-1}}$. Moreover, since v is prime, it follows that $\gcd(x_1 - x_2, v) = 1$ and hence by the extended Euclid algorithm, they know $\alpha, \beta \in \mathbb{Z}$ such that $\alpha(x_1 - x_2) + \beta v = 1$. Therefore, they know

$$a^{v^{-1}} = a^{v^{-1}(\alpha(x_1-x_2)+\beta v)} = M^\alpha a^\beta . \quad (1)$$

Next, from A_1 (or A_2), they compute

$$a^{y_1 v^{-1}} = \frac{A_1}{a^{x_1 v^{-1}}} = \frac{A_1}{(a^{v^{-1}})^{x_1}} \quad (2)$$

where $a^{v^{-1}}$ is given by Eq. (1).

Also, noting that $\gcd(x_1^2 - x_2^2, v) = 1$, they again use the extended Euclid algorithm to compute $\eta, \xi \in \mathbb{Z}$ such that $\eta(x_1^2 - x_2^2) + \xi v = 1$. So from $B_1 = b^{(x_1^2+y_2)v^{-1}}$ and $B_2 = b^{(x_2^2+y_2)v^{-1}}$, they compute

$$b^{v^{-1}} = (B_1/B_2)^\eta b^\xi \quad (3)$$

and

$$b^{y_2 v^{-1}} = \frac{B_1}{(b^{v^{-1}})^{x_1^2}} . \quad (4)$$

Once $a^{v^{-1}}$, $a^{y_1 v^{-1}}$, $b^{v^{-1}}$ and $b^{y_2 v^{-1}}$ are known, a new membership certificate can be computed as $(A, B) = ((a^{v^{-1}})^x a^{y_1 v^{-1}}, (b^{v^{-1}})^{x^2} b^{y_2 v^{-1}})$ for some arbitrary $0 < x < v$.

3 Conclusions

This report shows that the second group signature proposed by Ateniese and Tsudik does not present the required property, i.e., coalition-resistance.

Acknowledgments

The author is grateful to Giuseppe Ateniese for some pertinent remarks on a preliminary version of this report. Thanks also go to Markus Michels for showing that the (primary) fix suggested in an earlier version was not enough to resist against coalition attacks.

References

- [1] Giuseppe Ateniese and Gene Tsudik, *Group signatures à la carte*, To appear in Proc. of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '99), January 1999.
- [2] ———, *A coalition-resistant group signature*, Submitted, October 30, 1998.

- [3] Jan Camenisch, *Group signature schemes and payment systems based on the discrete logarithm problem*, Ph.D. thesis, ETH Zürich, Zurich, February 1998, Published in ETH Series in Information Security and Cryptography, vol. 2, Hartung-Gorre, 1998.
- [4] 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.
- [5] Lidong Chen and Torben Pryds Pedersen, *New group signature schemes*, Advances in Cryptology — EUROCRYPT '94 (A. De Santis, ed.), Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1995, pp. 171–181.
- [6] Anna Lysyanskaya and Zulfikar Ramzan, *Group blind signatures: A scalable solution to electronic cash*, Financial Cryptography (R. Hirschfeld, ed.), Lecture Notes in Computer Science, vol. 1465, Springer-Verlag, 1998.
- [7] Clauss P. Schnorr, *Efficient signature generation by smart cards*, Journal of Cryptology **4** (1991), no. 3, 161–174.