INFORMATICA, 2003, Vol. 14, No. 1, 85–94

On the Linkability of Some Group Signature Schemes

Hung-Min SUN,
Department of Computer Science, National Tsing Hua University
Hsinchu, Taiwan 300
e-mail: hmsun@cs.nthu.edu.tw

Her-Tyan YEH, Tzonelih HWANG
Department of Computer Science and Information Engineering
National Cheng Kung University
Tainan, Taiwan 701
e-mail: htyeh@ismail.csie.ncku.edu.tw

Received: March 2003

Abstract. A group signature scheme is a digital signature scheme that allows a group member to sign messages anonymously on behalf of the group. Recently, Tseng and Jan proposed two group signature schemes based on self-certified and ID-based public keys respectively. However, these two schemes were shown to be insecure against forgery due to Joye *et al.* Later, Sun *et al.* showed that Tseng and Jan's self-certified group signature scheme is linkable. In this paper, we first point out that the proposed linking equation, which is used to check the linkability of Tseng and Jan's self-certified scheme, cannot work because the inverse problem of RSA is hard. A repaired linking equation is consequently proposed to fix this problem. Then, we show that Tseng and Jan's ID-based scheme is still linkable because given any two valid group signatures it is easy to decide whether these two group signatures are generated by the same group member or not.

Key words: cryptography, group signatures, digital signatures, ID-based, self-certified, data security.

1. Introduction

Digital signatures are becoming more important in the industrial and commercial areas. It allows the owner of an electronic message to sign the message that everyone is able to verify the validity of the signature and no one can forge a valid signature on behalf of the signer.

Group signature (Chaum and van Heyst, 1993) is a digital signature that allows a group member to sign messages anonymously on behalf of the group. More formally, a group signature has the following properties:

1. Only the group members are able to sign on behalf of the group.
2. The receiver can verify that it is a valid signature of that group, but cannot distinguish which group member made the signature.

3. In case of disputes, the signature can be "opened" to reveal the identity of the signer.

So far, various group signature schemes have been proposed (Camenisch, 1997; Camenisch and Michels, 1998; Camenisch and Stadler, 1997; Chen and Pedersen, 1995; Lee and Chang, 1998; Petersen, 1998; Park *et al.*, 1997; Tseng and Jan, 1999b). Park *et al.* (1997) presented an ID-based group signature, which is based on the Ohta–Okamoto's ID-based signature scheme (Ohta and Okamoto, 1988). Their scheme suffers from the weakness that the size of a group signature is dependent upon the number of group members. Moreover, it has been shown in (Mao and Lim, 1998) that their scheme does not provide anonymity. In 1998, Lee and Chang (1998) suggested another efficient group signature scheme. However their scheme doesn't enjoy the desirable property of unlinkability and is insecure against some attacks (Joye *et al.*, 1999a). In order to provide the unlinkability property in Lee and Chang's scheme, Tseng and Jan (Tseng and Jan, 1999a) proposed an improved group signature scheme. Soon, the improved scheme was shown to be linkable due to Sun (1999) and be insecure against forgery due to Joye, Lee and Hwang (Joye *et al.*, 1999a). Recently, based on self-certified public keys (Saeednia, 1997; Wu *et al.*, 1998), Tseng and Jan (1999) proposed a group signature scheme using self-certified public keys. Later, Sun, Chen and Hwang showed that Tseng and Jan's scheme is linkable. In order to enhance the security and improve the performance of Park *et al.*'s scheme, Tseng and Jan (1999) further proposed a novel ID-based group signature scheme in which the size of a group signature is constant. However, these two group signature schemes (self-sertified and ID-based) proposed by Tseng *et al.* were shown to be insecure against forgery due to Joye, Kim and Lee (1999). In this paper, we first point out that the proposed linking equation, which is used to check the linkability of Tseng and Jan's self-certified scheme, cannot work because the inverse problem of RSA is hard. A repaired linking equation is consequently proposed to fix this problem. Then, we show that Tseng and Jan's ID-based scheme is still linkable because given any two valid group signatures it is easy to decide whether these two group signatures are generated by the same group member or not.

The rest of this paper is organized as follows. In Section 2, we briefly review Tseng and Jan's group signature schemes. In Section 3, we review the linkability of Tseng and Jan's self-certified group signature scheme. In Section 4, we comment on the linking equation, which is proposed by Sun, Chen and Hwang, and propose a repaired linking equation to fix this problem. In Section 5, we show the linkability of Tseng and Jan's ID-based group signature scheme. Finally, we conclude this paper in Section 6.

2. Review of Tseng and Jan's Group Signature Schemes

In this section, we give a short description of the Tseng–Jan group signature schemes. We refer the reader to (Tseng and Jan, 1999b; Tseng and Jan, 1999c) for more details.

These schemes involve four roles of participants: a trusted authority, a group authority, group members, and verifiers. The trusted authority is responsible for setting up system

parameters. The group authority is responsible for issuing membership certificates to new group members who join the group, and in case of a dispute for opening the contentious group signature to reveal the identity of the actual signer. The group members sign messages on behalf of the group, and the verifiers check the validity of the group signatures using the group public key.

Tseng and Jan's schemes are divided into three stages: the system setup stage, the group signature and verification stage, and the user identification stage.

2.1. *Self-Certified Group Signature Scheme*

2.1.1. *System Setup Stage*

This stage consists of the system initialization phase and the group creation phase.

System Initialization Phase. The trusted authority chooses: two large primes p and q of the same size and $N = pq$ such that $p = 2p' + 1$ and $q = 2q' + 1$ where p' and q' are also primes, a base $g \in Z_Z^*$ with order $v = p'q'$, and a large integer $u < v$. The trusted authority then selects an odd integer $e \in Z_v^*$ and computes the corresponding value d such that $e \cdot d = 1 \bmod v$. The parameters d, p, q, p', and q' are kept secret. The parameters e, N, g and u are made public.

When a user U_i (whose identity description is D_i) wants to join the system, he randomly selects his secret key $s_i \in Z_u$ and computes $g^{s_i} \bmod N$. Then he sends $g^{s_i} \bmod N$ and D_i to the trusted authority for requesting his public key. The trusted authority computes and publishes his public key as $p_i = g^{s_i \cdot ID_i^{-1} \cdot d} \bmod N$, where $ID_i = f(D_i)$. After getting the public key, the user can verify the validity of his public key by checking whether the equation: $p_i^{e \cdot ID_i} = g^{s_i} \bmod N$ holds.

Besides, there exists a group authority (whose identity description is GD) for setting up the group signature scheme. Similarly, the group authority randomly selects his secret key $x \in Z_u$ and computes $g^x \bmod N$, then sends $g^x \bmod N$ and GD to the trusted authority for requesting his public key. The trusted authority computes and publishes his public key as $y = g^{x \cdot GID^{-1}} \bmod N$, where $GID = f(GD)$. The group authority can verify the validity of his public key by checking whether the equation: $y^{GID} = g^x \bmod N$ holds. The trusted authority also computes another secret key for the group authority as $s_G = g^{-x \cdot d} \bmod N$ and sends it to the group authority secretly.

Group Creation Phase. The responsibility of the group authority is to create a group such that each member in this group can sign a message on behalf the group. Therefore, for each group member U_i with identity ID_i, the group authority computes $x_i = p_i^{ID_i \cdot x} \cdot s_G \bmod N (= g^{s_i \cdot d \cdot x} \cdot g^{-x \cdot d} \bmod N)$ as another secret key of U_i. The secret key x_i is transmitted to the group member U_i secretly. The group member U_i can verify the validity of the secret key by checking whether the equation: $x_i^e = y^{GID \cdot s_i} \cdot y^{-GID} \bmod N$ holds.

2.1.2. *Group Signature and Verification Stage*

When a group member U_i wants to sign a message M on behalf of the group, he first chooses three random integers r_1, r_2, and r_3 in Z_u. Then the group signature parameters $\{A, B, C, D, E\}$ are computed as follows.

$A = r_1 \cdot s_i$,
$B = r_2^{-e \cdot A} \bmod N$,
$C = \left(y^{GID \cdot A}\right)^{r_3} \bmod N$,
$D = s_i \cdot h\big(M \parallel A \parallel B \parallel C\big) + r_3 \cdot C$,
$E = x_i \cdot r_2^{h(M \| A \| B \| C \| D)} \bmod N$,
where '| |' denotes concatenation.

Thus the 6-tuple $\{M, A, B, C, D, E\}$ is a valid group signature.

Upon receiving the group signature $\{M, A, B, C, D, E\}$, anyone (verifier) can verify the validity of the signature by checking whether the following congruence holds:

$$\left(y^{GID \cdot A}\right)^D = \left(E^{e \cdot A} \cdot B^{h(M \| A \| B \| C \| D)} \cdot y^{GID \cdot A}\right)^{h(M \| A \| B \| C)} \cdot C^C \bmod N.$$

2.1.3. *User Identification Stage*

In the case of a later dispute, the group signature may be "opened" such that the identity of the signer is revealed. Because the group authority knows all of secret keys xi of the group members, for $i = 1, 2, ..., k$, where k is the number of the group members, the identity of the signer can be found by the equation

$$(x_i)^{e \cdot A} \cdot B^{-h(M \| A \| B \| C \| D)} = E^{e \cdot A} \bmod N.$$

If the equation holds, then xi is the secret key of the signer. In order to convince others, the group authority randomly selects an integer r in Z_u, and computes

$$R = ((p_i^{ID_i \cdot e} \cdot g^{-1})^A)^r \bmod N,$$
$$S = r + h(R \parallel M \parallel A \parallel B \parallel C \parallel D) \cdot x.$$

Then the group authority publishes the identification information (R, S) and the user's identity ID_i. Upon receiving the information from the group authority, anyone can identity the identity ID_i of the signer for the group signature $\{M, A, B, C, D, E\}$ by checking whether the following equation holds:

$$R \cdot \left(E^{e \cdot A} \cdot B^{h(M \| A \| B \| C \| D)}\right)^{h(R \| M \| A \| B \| C \| D)} = \left(p_i^{ID_i} \cdot g^{-1}\right)^{S \cdot A} \bmod N.$$

2.2. *ID-Based Group Signature Scheme*

2.2.1. *System Setup Stage*

System Initialization Phase. For setting up the system, the trusted authority selects two large primes p_1 ($\equiv 3 \bmod 8$) and p_2 ($\equiv 7 \bmod 8$) such that both $(p_1 - 1)/2$ and $(p_2 - 1)/2$ are odd and relatively prime. Note that with the above limitations for p_1 and p_2, it is feasible for the trusted authority to find the discrete logarithms for p_1 and p_2 (Lim and Lee, 1992; Maurer and Yacobi, 1992; Maurer and Yacobi, 1996). Let $N = p_1 p_2$. The trusted authority also selects two integers e and t in $Z^*_{\phi(N)}$ and computes the corresponding values d and v which satisfies

$ed \equiv 1(\mathrm{mod}\phi(N))$,

$vt \equiv 1(\mathrm{mod}\phi(N))$,

but keeps t, d, and v in secret and publishes e. Let g be a primitive element in Z_N^*. Then the trusted authority computes a public value

$F = g^v \mathrm{mod} N$,

where $v \equiv t^{-1}(\mathrm{mod}\phi(N))$.

When a user U_i (with identity information D_i) wants to join the group, the trusted authority computes:

$s_i = et \log_g ID_i \bmod \phi(N)$,

where

$$ID_i = \left\{ \begin{array}{c} D_i \bmod N \text{ if } D_i/N) = 1 \\ 2D_i \bmod N \text{ if}(D_i/N) = -1 \end{array} \right\}.$$

Finally, the trusted authority sends s_i to the user U_i secretly.

Group Creation Phase. Let GA be a group authority with secret key x and computes the corresponding public key $y = F^x \mathrm{mod} N$. For each group member U_i (with identity information ID_i), the group authority computes:

$x_i = ID_i^x \bmod N$.

Then, GA sends x_i to the user U_i secretly.

From the above phases, the system parameters are summarized as follows:

1. The secret values of the trusted authority are $(p_1; p_2; d; v; t; x)$.
2. The public values of the trusted authority are $(N; e; g; F; y)$.
3. The secret key of the group authority is x.
4. The public key of the group authority is y.
5. The secret key of the user U_i is the pair (s_i, x_i).
6. The public key of the user U_i is ID_i.

2.2.2. *Group Signature and Verification Stage*

When a group member U_i wants to sign a message M on behalf of the group, he first chooses two random integers r_1, r_2 in Z_N^*. Then the group signature (A, B, C, D) for the message M is computed as follows.

$A = y^{r_1} \bmod N$,

$B = y^{r_2 \cdot e} \bmod N$,

$C = s_i + r_1 \cdot h\,(M \parallel A \parallel B) + r_2 \cdot e$,

$D = x_i \cdot y^{r_2 \cdot h(M \| A \| B \| C)} \bmod N$,

where '$\|$' denotes concatenation and $h()$ is a one-way hash function.

Upon receiving the group signature (A, B, C, D) on the message M, anyone (verifier) can verify the validity of the group signature by checking whether the following congruence holds:

$D^e \cdot A^{h(M \| A \| B)} = y^C \cdot B^{h(M \| A \| B \| C)} \bmod N$.

2.2.3. *User Identification Stage*

In case of a dispute, the group authority can open the group signature in order to know who indeed signs the group signature by finding ID_i satisfying the following equation:

$$(ID_i)^{x \cdot e} = D^e \cdot B^{-h(M\|A\|B\|C)} \bmod N$$

for $i = 1 \ldots k$, where k is the number of the group numbers.

In order to convince other verifiers that the user U_i with identity ID_i is indeed the signer, the group authority randomly selects an integer r in Z_N^*, and computes

$R = (ID_i)^{r \cdot e} \bmod N$,

$S = r + h(M \parallel A \parallel B \parallel R) \cdot x$.

Then the group authority publishes the identification information (R, S) and the user's identity ID_i. Upon receiving the announcement from the authority, the verifier may identify the identity ID_i of the signer for the group signature (A, B, C, D) by checking the following equation

$$(ID_i)^{S \cdot e} = R \cdot \left(y^C \cdot A^{-h(M\|A\|B)} \cdot B^{-1}\right)^{h(M\|A\|B\|R)} \bmod N.$$

If the above equation holds, the user with the identity ID_i is identified.

3. Review of Linkability of Tseng and Jan's Self-Certified Group Signature Scheme

One of the main properties of group signatures is allowing the group members to anonymously sign on behalf of the group. This property is called unlinkability. I. e., two valid different group signatures are unlinkable if no one (but the group authority) can decide whether these two signatures were generated by the same group member or not.

In this following, we review Sun *et al.*'s attack (Sun *et al.*, 1999) that Tseng and Jan's self-certified scheme is linkable, i.e., given two group signatures, it can be easily decided if both signatures are generated by the same group member.

Without loss of generality, we assume that $\{M, A, B, C, D, E\}$ and $\{M', A', B', C', D', E'\}$ are two valid group signatures. If the same group member U_i generates these two group signatures, then from the signature generation stage we know:

$$B^{A^{-1} \cdot h(M\|A\|B\|C\|D)} = r_2^{-e \cdot h(M\|A\|B\|C\|D)} \bmod N, \tag{1}$$

$$E^e = x_i^e \cdot r_2^{e \cdot h(M\|A\|B\|C\|D)} \bmod N, \tag{2}$$

$$(B')^{(A')^{-1} \cdot h(M'\|A'\|B'\|C'\|D')} = (r_2')^{-e \cdot h(M'\|A'\|B'\|C'\|D')} \bmod N, \tag{3}$$

$$(E')^e = x_i^e \cdot (r_2')^{e \cdot h(M'\|A'\|B'\|C'\|D')} \bmod N. \tag{4}$$

Let (1) multiply (2), we obtain:

$$B^{A^{-1} \cdot h(M\|A\|B\|C\|D)} \cdot E^e = x_i^e \bmod N. \tag{5}$$

Similarly, let (3) multiply (4), we obtain:

$$(B')^{(A')^{-1}\cdot h(M'\|A'\|B'\|C'\|D')} \cdot (E')^e = x_i^e \bmod N. \tag{6}$$

From (5) and (6), we know:

$$B^{A^{-1}\cdot h(M\|A\|B\|C\|D)} \cdot E^e = (B')^{(A')^{-1}\cdot h(M'\|A'\|B'\|C'\|D')} \cdot (E')^e \bmod N. \tag{7}$$

Thus the proposed group signature scheme is linkable by checking whether (7) holds (note that e is public). That is, if (7) holds, then these two group signatures come from the same signer, and vice verse.

4. Comment and Repair of Sun, Chen and Hwang's Attack

4.1. *Comments on the Linking Equation*

In fact, the linking equation (7) cannot work because both $A^{-1} \bmod \phi(N)$ and $(A')^{-1} \bmod \phi(N)$ are unknown to any verifier due to the difficulty of factoring N. This is similar to the inverse problem of RSA that one who knows the public exponent is infeasible to compute the secret exponent.

4.2. *A Repaired Linking Equation*

We need only raise AA' to two sides of the linking (7). Thus we can obtain the following linking equation:

$$\begin{aligned} &B^{A^{-1}\cdot h(M\|A\|B\|C\|D)} \cdot E^{A(A')e} \\ &\quad = (B')^{(A')^{-1}\cdot h(M'\|A'\|B'\|C'\|D')} \cdot (E')^{A(A')e} \bmod N. \end{aligned} \tag{8}$$

This linking equation (8) is feasible because the inverse problem of RSA no longer exists in this equation.

5. Linkability of Tseng and Jan's ID-Based Group Signature Scheme

In this following, we apply the model of Sun, Chen and Hwang's attack to show that Tseng and Jan's ID-based scheme is still linkable because given two valid group signatures, it can be easily decided if the same group member generates both signatures.

We assume that (A, B, C, D) and (A', B', C', D') are two valid group signatures. From the signature generation stage we know:

$$B^{h(M\|A\|B\|C)} = y^{r_2\cdot h(M\|A\|B\|C)} \bmod N, \tag{9}$$

$$D^e = x_i^e \cdot y^{r_2\cdot e\cdot h(M\|A\|B\|C)} \bmod N, \tag{10}$$

$$(B')^{h(M'\|A'\|B'\|C')} = y^{r_2^{'}\cdot h(M'\|A'\|B'\|C')} \bmod N, \tag{11}$$

$$(D')^e = (x_i^{'})^e \cdot y^{r_2^{'}\cdot e\cdot h(M'\|A'\|B'\|C')} \bmod N. \tag{12}$$

From (9) and (1)0, we obtain:

$$B^{h(M\|A\|B\|C)} \cdot x_i^e = D^e \bmod N. \tag{13}$$

Similarly, from (11) and (12), we obtain:

$$(B')^{h(M'\|A'\|B'\|C')} \cdot (x_i^{'})^e = (D')^e \bmod N. \tag{14}$$

From (13) and (14), we know:

$$B^{h(M\|A\|B\|C)} \cdot (D')^e \cdot x_i^e = (B')^{h(M'\|A'\|B'\|C')} \cdot D^e \cdot (x_i^{'})^e \bmod N. \tag{15}$$

If these two group signatures are generated by the same group member, then x_i is equal to $x_i^{'}$. So, in this case, (15) can be reduced into:

$$B^{h(M\|A\|B\|C)} \cdot (D')^e = (B')^{h(M'\|A'\|B'\|C')} \cdot D^e \bmod N. \tag{16}$$

Since no secret parameter is included in (16), we can check whether (16) holds or not. If (16) holds, then these two group signatures come from the same signer. If (16) doesn't hold, then these two group signatures come from different group members. So, Tseng and Jan's group signature scheme is linkable. In the following, we give an example to illustrate the point about the linkability.

Example. Let $p' = 3$, $q' = 5$, $p = 2p' + 1 = 7$, $q = 2q' + 1 = 11$, $N = pq = 77$, $e = 7$, $d = 13$, $ed \equiv 1 \bmod p'q'$. Two group signatures $(A, B, C, D) = (3, 2, 5, 2)$, $(A', B', C', D') = (11, 13, 7, 3)$. Let $h(M \parallel A \parallel B \parallel C) = 2$, $h(M' \parallel A' \parallel B' \parallel C') = 1$. We can find $B^{h(M\|A\|B\|C)} \cdot (D')^e \bmod N = 2^2 \cdot 3^7 \bmod 77 = 47$, and $(B')^{h(M'\|A'\|B'\|C')} \cdot D^e \bmod N = 13^1 \cdot 2^7 \bmod 77 = 47$. By (16), we can decide that these two group signatures come from the same signer.

6. Conclusions

In this paper, we first point out that the proposed linking equation, which is used to check the linkability of Tseng and Jan's self-certified scheme, cannot work because the inverse problem of RSA is hard. A repaired linking equation is consequently proposed to fix this problem. Then, we show that Tseng and Jan's ID-based scheme still suffers from the weakness of linkability.

References

Camenisch, J. (1997). Efficient and generalized group signatures. *Advances in Cryptology EUROCRYPT '97*, *LNCS*, **1233**, 465–479.

Camenisch, J., and M. Michels (1998). A group signature scheme based on an RSA variant. BRICS report, preliminary version in *Advances in Cryptology – ASIACRYPT '98*, *LNCS*, **1514**, 160–174.

Camenisch, J., and M. Stadler (1997). Efficient group signature schemes for large groups. *Advances in Cryptology – CRYPTO '97*, *LNCS*, **1296**, 410–424.

Chaum, D., and E. van Heyst (1993). Group signatures. *Advances in Cryptology – EUROCRYPT'91*, *LNCS*, **547**, 257–265.

Chen, L., and T.P. Pedersen (1995). New group signature schemes. In *Advances in Cryptology – EUROCRYPT'94*. pp. 163–173.

Joye, M., N.Y. Lee and T. Hwang (1999a). *On the security of the Lee–Chang group signature scheme and its derivatives*, *Information Security Workshop*.

Joye, M., S. Kim and N.Y. Lee (1999b). Cryptanalysis of two group signature schemes. In M. Mambo and Y. Zheng (Eds.), *Information Security, Lecture Notes in Computer Science*, Vol. 1729. pp. 271–275.

Lee, W.B., and C.C. Chang (1998). Efficient group signature scheme based on the discrete logarithm. In *IEE Proc. Comput. Digit. Tech.*, **145**(1). pp. 15–18.

Lim, W.B., and P.J. Lee (1992). Modified Maurer–Yacobi's scaeme and its application. In *Proc. AUSCRYPT'91*. pp. 308–323.

Mao, W., and C.H. Lim (1998). Cryptanalysis in prime order subgroups of Zn. *Advances in Cryptology – ASIACRYPT'98*, *LNCS*, **1514**, 214–226.

Maurer, U.M., and Y. Yacobi (1992). Non-interactive public-key Cryptography. In *Proc. EUROCRYPT'91*. pp. 498–507.

Maurer, U.M., and Y. Yacobi (1996). A non-interactive public-key distribution system. *Designs, Codes and Cryptography*, **9**, 305–316.

Ohta, K., and E. Okamoto (1988). Practical extension of Fiat–Shamir scheme. *Electronics Letters*, **24**(15), 955–956.

Petersen, H. (1998). How to convert any digital signature scheme into a group signature. *Security Protocols Workshop*, *LNCS*, **1361**.

Park, S., S. Kim and D. Won (1997). ID-based group signature. *Electronics Letters*, **33**(19), 1616–1617.

Saeednia, S. (1997). Identity-based and self-certified key-exchange protocols. In *Proc. Information Security and Privacy, Second Australasian Conf.*, Sydney, Australia. pp. 303–313.

Sun, H.M. (1999). Comments on improved group signature scheme based on the discrete logarithm. *IEE Electronics Letters*, **35**(16), 1323–1324.

Sun, H.M., B.J. Chen and T. Hwang (1999). Cryptanalysis of group signature scheme using self-certified public keys. *Electronics Letters*, **35**(22), 1938–1939.

Tseng, Y.M., and J.K. Jan (1999a). Improved group signature scheme based on the discrete logarithm. *Electronics Letters*, **35**(1), 37–38.

Tseng, Y.M., and J.K. Jan (1999b). A group signature scheme using self-certified public keys. In *Proc. of the Ninth National Conference on Information Security*. pp. 165–172.

Tseng, Y.M., and J.K. Jan (1999c). A novel ID-based group signature. *Information Sciences*, **120**, 131–141.

Wu, T.C., Y.S. Chang and T.Y. Lin (1998). Improvement of Saeednia's self-certified key exchange protocols. *Electronics Letters*, **34**(11), 1094–1095.

H.-M. Sun received his B.S. degree in applied mathematics from National Chung–Hsing University in 1988, his M.S. degree in applied mathematics from National Cheng Kung University in 1990, and his Ph.D. degree in computer science and information engineering from National Chiao–Tung University in 1995, respectively. He was an associate professor with the Department of Information Management, Chaoyang University of Technology from 1995 to 1999, and the Department of Computer Science and Information Engineering, National Cheng Kung University from 1999 to 2002. Currently he is an associate professor with the Department of Computer Science, National Tsing Hua University. He has published over seventy papers. He was the program chair of 2001 National Information Security Conference and the program committee member of 1997 Information Security Conference, 2000 Workshop on Internet and Distributed Systems, Workshop on the 21st Century Digital Life and Internet Technologies, 1998 and 1999 National Conference on Information Security. His research interests include cryptography, information theory, network security, image compression.

H.-T. Yeh was born in Tainan, Taiwan, in 1965. He received his B.S. degree in Information Science from Soochow University in 1989 and M.S. degrees in Computer Science and Information Engineering from Nation Taiwan University in 1996. Now, he is currently pursuing his Ph.D. degree in Institute of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan.

T. Hwang was born in Tainan, Taiwan ROC in March, 1958. He received his undergraduate education from National Cheng Kung University, Taiwan ROC in 1980 and the M.S. and Ph.D. degrees in Computer Science from the University of Southwestern Louisiana USA in 1988. He is presently a professor of the Department of Information Engineering, National Cheng Kung University, Taiwan ROC. His research interests include cryptology, network security and coding theory. Dr. Hwang is a member of IEEE and also a member of International Association for Cryptographic Research.

Apie kai kurių grupės parašų atskiriamumą

Hung-Min SUN, Her-Tyan YEH, Tzonelih HWANG

Grupės parašas yra skaitmeninis parašas, kuris leidžia grupės nariui pasirašyti pranešimus anonimiškai grupės vardu. Neseniai Tseng ir Jan pasiūlė du grupės parašo metodus, pagrįstus sertifikatais ir vartotojo tapatybe nustatančiais viešaisiais raktais. Tačiau Joye *et al.* įrodė, jog šie du metodai yra nesaugūs klastojimui. Vėliau Sun *et al.* parodė, kad Tseng ir Jan sertifikuotas grupės parašas yra atskiriamas. Šiame straipsnyje parodoma, kad siūloma atskyrimo lygtis, kuri yra naudojama patikrinti Tseng ir Jan sertifikavimo metodą, negali veikti, kadangi atvirkštinė RSA problema yra sudėtinga. Šiai problemai spręsti siūloma pataisyta atskiriamumo lygtis. Tuomet parodoma, kad Tseng ir Jan vartotojo tapatybe pagrįstas metodas yra atskiriamas, kadangi, turint bet kuriuos du galiojančius grupės parašus, lengva nuspręsti, ar šie parašai yra sukurti to paties grupės nario, ar ne.