

Short Paper

(t, n) Threshold Untraceable Signatures

NARN-YIH LEE*, TZONELIH HWANG AND CHUAN-MING LI

**Department of Applied Foreign Language
Southern Taiwan University of Technology
Tainan, Taiwan 710, R.O.C.*

*E-mail: nylee@mail.stut.edu.tw
Institute of Information Engineering
National Cheng-Kung University
Tainan, Taiwan 701, R.O.C.
E-mail: hwangtl@server2.iie.ncku.edu.tw*

A (t, n) threshold signature scheme is one which enables any t or more shareholders to cooperatively generate a group signature. Based on the traceability of the signers, threshold signatures can further be classified into (1) threshold traceable signatures, where the identities of the signers, who generate the signature, can be traced by the system; and (2) threshold untraceable signatures, where the signers of a signature cannot be traced. This paper distinguishes the applications of threshold signatures of both types and also proposes a threshold untraceable signature scheme. The new signature scheme can be augmented to give the original signers the ability to prove that they are the true signers.

Keywords: threshold signature scheme, multi-signature scheme, lagrange interpolating polynomial, RSA scheme, untraceability

1. INTRODUCTION

Digital signatures on electronic documents are widely used to replace hand written signatures on paper documents. The responsibility of signing a signature may have to be shared by a set of signers from time to time. For example, a company may require that any policy decision must be signed by at least t directors before it is issued. Shared signatures of this type are called *threshold signatures* [3, 7, 9]. Threshold signature schemes generate a signature for a group. Therefore, they differ from multi-signature schemes [8, 11, 12] in that threshold signatures can be verified without the verifier knowing the identities of signers by the verifier.

Based on the traceability of the signers, threshold signature schemes can be further classified into threshold traceable signature schemes and threshold untraceable signature schemes. Consider a log of inputs, which are required to be signed by at least t members in

Received September 24, 1998; revised April 12, 1999; accepted July 23, 1999.
Communicated by Chi Sung Laih.

a group. What the verifiers care about is that the signatures be generated from that group and signed by at least t members. They do not care about who the signers are. However, the system of that log of inputs may wish to identify the signers if a forged document, which is not from that input log, was signed. In this case, threshold *traceable* signatures [3, 7, 9], where the identities of the signers can be traced, have to be used.

On the other hand, in a democratic society, a proposal may have to be approved (signed) by at least t members of a group. For reasons of privacy and safety, the identities of the signers should be anonymous as far as both the system and the verifier are concerned under all circumstances. It is the threshold number of signers that is important rather than the identities of the signers of the proposal. Under this guarantee, the members of that group will be able to fulfill their responsibility freely. In this case, threshold *untraceable* signature schemes, where the signers cannot be traced, have to be used.

In the threshold untraceable signature schemes, the original signers may sometimes wish to prove that they are the true signers after a period of time. It is quite useful for the signers to have this option.

Desmedt and Frankel [3] proposed the first (t, n) threshold signature scheme in 1991. Later, Harn [7] combined the secret sharing scheme and the modified El-Gamal signature scheme [4] to construct another (t, n) threshold signature scheme. Basically, both schemes are traceable. This paper will attempt to propose a threshold untraceable signature scheme. First, we will present the properties of a threshold untraceable signature scheme.

- (1) The system should satisfy the properties of a threshold scheme; i.e., the group secret key S can be divided into n different “*secret shares*”, s_1, s_2, \dots, s_n , such that:
 - a.** a group signature can be easily produced with knowledge of at least t secret shares ($t \leq n$);
 - b.** it is impossible to generate a group signature with knowledge of $t - 1$ or fewer secret shares;
 - c.** the group secret key cannot be derived from the released group signature or partial signatures; and
 - d.** it is impossible to derive any secret share from the released group signature or partial signatures.
- (2) It is better that the size of the group signature be equivalent to the size of an individual signature.
- (3) The group signature can be verified by any outsider without the need to identify the identities of the signers, and the verification process should be as simple as possible.
- (4) The signers of the group signature cannot be traced.

The rest of this paper is organized as follows. In the next section, a modified digital signature scheme based on Ohta and Okamoto’s signature scheme [10] will be described. In section 3, a (t, n) threshold untraceable signature scheme will be devised based on the modified signature scheme. Then, the proposed (t, n) threshold untraceable signature scheme will be further modified to have the property that the original signers can prove they are the true signers. Finally, concluding remarks will be made in section 4.

2. MODIFIED DIGITAL SIGNATURE SCHEME

In 1988, Ohta and Okamoto [10] proposed a digital signature scheme based on the Fiat-Shamir scheme [5]. The Ohta and Okamoto signature scheme [10] will be slightly modified here to construct a threshold untraceable signature scheme. The modified signature scheme is described in the following.

Each user i in the system first selects two large random primes, p and q , and computes N using $N = pq$. For p and q to be safe primes, let $p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are also primes [1, 2]. Define $\lambda(N) = 2p'q'$. (λ is the Carmichael function, i.e., the exponent of Z_N^* .) Let L be a random number (e.g., $L \approx 10^{50}$), and let $GCD(L, \lambda(N)) = 1$. User i selects a secret random number s , $1 \leq s \leq \lambda(N)$ and an element α which is primitive in both $GF(p)$ and $GF(q)$. User i computes

$$K_i = \alpha^s \text{ mod } N$$

as his secret key and computes

$$Y_i = \alpha^{sL} \text{ mod } N$$

as his public key. In summary, the secret keys of user i are p , q and K_i , and the public keys of user i are N , L and Y_i .

Let $g(\cdot)$, be a collision free one-way hash function [15]. To generate a signature for the message M ($1 \leq M \leq N - 1$), the signer, user i , chooses a random number r between 1 and $N - 1$. Then, the user computes

$$\begin{aligned} u &= r^L \text{ mod } N, \\ e &= g(u, M), \text{ and} \\ z &= r \cdot K_i^e \text{ mod } N. \end{aligned}$$

(e, z) is the signature of the message M .

To verify the validity of the signature (e, z) , the verifier uses user i 's public keys, Y_i , L and N , to compute a value \bar{u} as

$$\bar{u} = z^L \cdot Y_i^e \text{ mod } N.$$

Then, the verifier checks

$$e \stackrel{?}{=} g(\bar{u}, M).$$

If the above equation holds, then the signature (e, z) is valid.

Discussion: It is noted here that there are other signature schemes of the same type, e.g., the Guillou and Quisquater signature scheme [6], which can also be modified in the same way to construct threshold untraceable signature schemes.

In the Ohta and Okamoto signature scheme [10], user i randomly selects a secret number s as his secret key and computes the corresponding public key $Y_i = s^{-L} \bmod N$. However, in the modified signature scheme, user i uses $K_i (= \alpha^s \bmod N)$ and $Y_i (= K_i^{-L} \bmod N)$ as his secret and public key, respectively. The security of the modified signature scheme is the same as that of the Ohta and Okamoto signature scheme.

3. (t, n) THRESHOLD UNTRACEABLE SIGNATURE SCHEMES

3.1 The Scheme

In this subsection, a (t, n) threshold untraceable signature scheme will be devised based on the modified digital signature scheme. The (t, n) threshold untraceable signature scheme is described in three phases in the following.

Phase 1: Group Secret Key and Secret Shares Generation Phase

Assume that there is a share distribution center (SDC) responsible for distributing keys for the system. Let A ($|A| = n$) be the set of all shareholders in the system. B ($|B| = t$) ($t \leq n$), any subset of size t in A , is authorized to generate a signature for a message.

SDC selects the system parameters N, p, q, p', q', α and L as in section 2. Both N and L are published while p, q, p', q' and $\lambda(N)$ are kept secret.

SDC next computes the group secret key S and public key Y as follows:

$$S = \alpha^d \bmod N,$$

where d is a random such that $GCD(d, \lambda(N)) = 1$ (so d is odd);

$$Y = \alpha^{-dL} \bmod N.$$

SDC randomly generates a secret polynomial $f(x)$ modulo $\lambda(N)$ of degree $t - 1$ and $f(0) = d$.

Finally, the SDC distributes to each shareholder $i, i \in A$, a public odd integer x_i with even $f(x_i)$ [3], and a secret key $K_i = \alpha^{s_i} \bmod N$, where

$$s_i = \frac{f(x_i)/2}{\left(\prod_{\substack{j \in A \\ j \neq i}} (x_i - x_j) \right) / 2} \pmod{p'q'}.$$

The SDC can be revoked after issuing these secret shares to the shareholders.

Phase 2: Partial Signature Generation Phase

Suppose B wishes to generate a signature for the message M . Each shareholder $i \in B$ has to generate a partial signature for M as follows.

User i chooses a random integer r_i between 1 and $N-1$, and computes a value $u_i = r_i^L \pmod N$. u_i is broadcast to all users in B . Once all u_i 's, $i \in B$, are available, user i computes the product U and a hash value e as

$$U = \prod_{i \in B} u_i \pmod N = R^L \pmod N,$$

$$e = g(U, M),$$

where $R = \prod_{i \in B} r_i \pmod N$.

The partial signature z_i can then be generated by user i :

$$z_i = r_i \cdot K_i^{\prod_{\substack{j \in A \\ j \neq i}} (x_i - x_j) \prod_{\substack{j \in B \\ j \neq i}} (0 - x_j) \cdot e} \pmod N.$$

Each user i in B sends the partial signature, $\{M, z_i\}$, to a designated combiner DC , who is responsible for collecting all partial signatures and producing the group signature. Since no secret information is kept, DC can be anyone in the system.

Phase 3: Group Signature Generation and Verification Phase

Upon receiving these t partial signatures, DC can compute Z as follows:

$$Z = \prod_{i \in B} z_i \pmod N$$

$$= R \cdot \alpha^{d \cdot e} \pmod N,$$

where $d = f(0) = \sum_{i \in B} s_i \prod_{\substack{j \in A \\ j \neq i}} (x_i - x_j) \prod_{\substack{j \in B \\ j \neq i}} (0 - x_j) \pmod{\lambda(N)}$ [3, 14]. $\{e, Z\}$ is the group signature of M .

To verify the validity of the group signature $\{e, Z\}$ for the message M , the verifier computes a value U as follows:

$$U = Z^L \cdot Y^e \pmod N.$$

Then, the verifier checks

$$e \stackrel{?}{=} g(U, M).$$

If the above equation holds, then the group signature $\{e, Z\}$ on the message M is valid.

Discussions: It is noted here that in Phase 2, DC does not have to verify the validity of the partial signature. If a faulty signature is presented, then the group signature cannot be successfully verified by the verifier. Shamir's (t, n) threshold scheme has been demonstrated to encounter the cheating problem in practice [16]. The last user has the advantage of being able to cheat the others without being detected. The proposed scheme is also threaten by this kind of attack. Thus, one can apply the methods in [16-19] to provide the capability of cheating detection or cheater identification.

In the new scheme, t or more shareholders are entitled to reveal the group secret key (α^d). However, they are unable to find the system secrets (p , q and d) or the secret keys (K_j 's) of all other shareholders.

Remark 1. One of the anonymous referees pointed out that the scheme in [7] can be a (t, n) threshold untraceable signature scheme if the scheme does not provide a partial signature verification mechanism.

Theorem 1: The proposed scheme is a (t, n) threshold signature scheme.

Proof: Since

$$e = g(U, M) = g(\prod_{i \in B} u_i, M) = g(\prod_{i \in B} r_i^L, M) = g(R^L, M),$$

where $R = \prod_{i \in B} r_i \pmod N$, and

$$\begin{aligned} z_i &= r_i \cdot K_i^{\prod_{j \in A} (x_i - x_j) \prod_{j \in B, j \neq i} (0 - x_j) \cdot e} \pmod N \\ &= r_i \cdot \alpha^{\prod_{j \in A} (x_i - x_j) \prod_{j \in B, j \neq i} (0 - x_j) \cdot e} \pmod N \\ &= r_i \cdot \alpha^{\frac{f(x_i)}{\prod_{j \in A, j \neq i} (x_i - x_j)} \cdot \prod_{j \in A} (x_i - x_j) \prod_{j \in B, j \neq i} (0 - x_j) \cdot e} \pmod N \\ &= r_i \cdot \alpha^{\prod_{j \in B, j \neq i} \frac{(0 - x_j)}{(x_i - x_j)} \cdot e} \pmod N, \end{aligned} \tag{1}$$

we have

$$\begin{aligned} Z &= \prod_{i \in B} z_i \pmod N \\ &= \prod_{i \in B} r_i \cdot \alpha^{\sum_{i \in B} \prod_{j \in B, j \neq i} \frac{(0 - x_j)}{(x_i - x_j)} \cdot e} \pmod N \end{aligned} \tag{2}$$

By using the secret sharing scheme [14], the unique $(t - 1)$ -th degree polynomial, $f(x)$, can be determined with knowledge of t pairs of $(x_i, f(x_i))$ by as follows:

$$f(x) = \sum_{i \in B} f(x_i) \cdot \prod_{\substack{j \in B \\ j \neq i}} \frac{x - x_j}{x_i - x_j} \pmod{\lambda(N)}. \tag{3}$$

Thus,

$$\begin{aligned} Z &= \prod_{i \in B} r_i \cdot \alpha^{\sum_{i \in B} \prod_{\substack{j \in B \\ j \neq i}} \frac{(0 - x_j)}{(x_i - x_j)} \cdot e} \pmod N \\ &= R \cdot \alpha^{f(0) \cdot e} \pmod N \\ &= R \cdot \alpha^{d \cdot e} \pmod N, \end{aligned}$$

where $d = f(0) = \sum_{i \in B} f(x_i) \cdot \prod_{j \neq i} \frac{0 - x_j}{x_i - x_j} \pmod{\lambda(N)}$.

Consequently,

$$\begin{aligned} U &= Z^L \cdot Y^e \pmod{N} \\ &= (R \cdot \alpha^{d \cdot e})^L \cdot \alpha^{d \cdot L \cdot e} \pmod{N} \\ &= R^L \pmod{N}. \end{aligned}$$

Therefore, as long as

$$\begin{aligned} e &= g(U, M), \text{ and} \\ U &= Z^L \cdot Y^e \pmod{N}, \end{aligned}$$

$\{e, Z\}$ must be a signature generated by an authorized group B of size at least t . \square

Theorem 2: The proposed (t, n) threshold signature scheme is untraceable.

Proof: Let $B' (\neq B)$ be any subset in A with $|B'| = t$. B' claims that the partial signatures z_i 's ($i = 1, \dots, t$) and the group signature (Z, e) are generated by the users i 's in B' .

To show the untraceability of the proposed threshold signature scheme, it is sufficient to show that the pair (r'_i, u'_i) generated by user i' in B' is indistinguishable from (r_i, u_i) originally generated by user i in B .

User i' in B' can compute r'_i and u'_i from the partial signature z_i as follows:

$$r'_i = z_i \cdot \left(\prod_{\substack{j \in A \\ j \notin B'}}^{(x_i - x_j)} \prod_{\substack{j \in B' \\ j \neq i}}^{(0 - x_j) \cdot e} \right)^{-1} \pmod{N},$$

and

$$u'_i = r_i'^L \pmod{N}.$$

Since the group signature Z can be expressed as

$$\begin{aligned} Z &= \prod_{i \in B} z_i \pmod{N} \\ &= \prod_{i \in B} r_i \cdot \prod_{\substack{j \in A \\ j \in B}}^{(x_i - x_j)} \prod_{\substack{j \in B \\ j \neq i}}^{(0 - x_j) \cdot e} \pmod{N} \\ &= \prod_{i \in B} r_i' \cdot \prod_{\substack{j \in A \\ j \in B'}}^{(x_i - x_j)} \prod_{\substack{j \in B' \\ j \neq i}}^{(0 - x_j) \cdot e} \pmod{N} \end{aligned}$$

and

$$\alpha^d = \alpha^{f(0)} = \prod_{i \in B} K_i^{\prod_{\substack{j \in A \\ j \in B}}^{(x_i - x_j)} \prod_{\substack{j \in B \\ j \neq i}}^{(0 - x_j)}} = \prod_{i \in B'} K_i^{\prod_{\substack{j \in A \\ j \in B'}}^{(x_i - x_j)} \prod_{\substack{j \in B' \\ j \neq i}}^{(0 - x_j)}}$$

mod N , this implies that the products $\prod_{i \in B} r_i \bmod N$ and $\prod_{i \in B} u_i \bmod N$ should be equivalent to the products $\prod_{i \in B'} r'_i \bmod N$ and $\prod_{i \in B'} u'_i \bmod N$, respectively. \square

3.2 Security Analysis

Theorem 1 shows that any subset of t shareholders ($t \leq n$) can generate a group signature. The group signature can also be verified easily by any verifier. In the following, several possible attacks will be investigated to demonstrate the security of the new system.

1. The group secret key S and the secret share K_i , $i \in A$, cannot be derived from the group public keys Y and N and the public parameter L .

To derive the group secret key S from the group public key $Y = S^L \bmod N$, the attacker faces the difficulty of breaking the RSA scheme [13]. Moreover, it is infeasible for an attacker to derive the secret share K_i if the secret polynomial $f(x)$ is unknown.

2. The group secret key S and the secret share K_i cannot be computed from a valid signature $\{e, Z\}$ and the partial signature z_i , $i \in B$, of the message M .

In order to reveal the group secret key S from Z , the attacker should first find out what the random product R is. Then, he calculates the e -th roots of $(Z \cdot R^{-1}) \bmod N$. However, retrieving R from U is as difficult as breaking the RSA scheme. Moreover, the difficulty of extracting the e -th roots of $(Z \cdot R^{-1}) \bmod N$ is equivalent to breaking the RSA scheme when $GCD(e, \lambda(N)) = 1$ and equivalent to factoring N if $GCD(e, p-1) \neq 1$ or $GCD(e, q-1) \neq 1$ [10]. In order to get the secret share K_i from the partial signature z_i , the attacker should first find out what r_i is. Then, he calculates the $\prod_{\substack{j \in A \\ j \neq B}} (x_i - x_j) \cdot \prod_{\substack{j \in B \\ j \neq i}} (0 - x_j) \cdot e$ -th roots of $(z_i \cdot r_i^{-1}) \bmod N$. However, retrieving r_i from $u_i = r_i^L \bmod N$ is equivalent to breaking the RSA scheme. Furthermore, let $V = \prod_{\substack{j \in A \\ j \neq B}} (x_i - x_j) \cdot \prod_{\substack{j \in B \\ j \neq i}} (0 - x_j) \cdot e$. The extraction of V -th roots mod N is as difficult as factoring N because $GCD(V, p-1) \neq 1$ and $GCD(V, q-1) \neq 1$. Thus, these attacks cannot work successfully.

3. One cannot impersonate a shareholder i , $i \in B$.

An attacker may try to impersonate a shareholder i , $i \in B$, by randomly selecting an integer $r'_i \in [1, N-1]$ and broadcasting $u'_i = r_i'^L \bmod N$. Since the productive value,

$U' = \left(\prod_{\substack{j \in B \\ j \neq i}} u_j \right) \cdot u'_i \bmod N$, is determined by all t these members in B and the hash value, e' , is obtained by $g(U', M)$, without knowledge of the secret share, K_i , it is difficult to generate a valid value z'_i satisfying the following equation:

$$z_i'^L \cdot \prod_{\substack{j \in B \\ j \neq i}} z_j^L = U' \cdot Y^{-e'} \bmod N.$$

4. t or more shareholders cannot collude to retrieve the system secrets.

To reconstruct the secret polynomial $f(x)$ of degree $t - 1$, at least t distinct $(x_i, f(x_i))$ pairs have to be collected. Since SDC distributes $K_i = \alpha^{s_i} \bmod N$ instead of s_i to the shareholder i , the problem for user i of deriving s_i from K_i is as difficult as the problem of solving the discrete logarithm modulo a composite number if α is known. (Furthermore, α may not be a public value in our scheme.) Therefore, any t or more shareholders cannot conspire to reconstruct the $\lambda(N)$ or the secret polynomial $f(x)$.

5. The group signature $\{e, Z\}$ for the message M cannot be forged.

An attacker may try to forge the signature of M by randomly selecting an integer R and then computing the $U = R^L \bmod N$ and the hash value $e = g(U, M)$. However, the group secret key S is unknown to the attacker. Solving Z such that $Z^L = U \cdot (Y^e)^{-1} \bmod N$ is as difficult as breaking the RSA scheme. On the other hand, the attacker may also try to randomly select a signature (e, Z) and compute $U = Z^L \cdot Y^e \bmod N$. However, it is infeasible to find a message M' such that $e = g(U, M')$ because $g()$ is a collision free one-way hash function. Any t or more shareholders cannot impersonate the other sets of shareholders to generate the group signature for the message M because these malicious shareholders cannot compute the system secrets and the secret keys of all shareholders.

6. The random numbers r_i 's or $R (= \prod_{i \in B} r_i)$ should be kept secret.

Given two different random numbers R_1 and R_2 and the corresponding signatures (e_1, Z_1) and (e_2, Z_2) , the following two equations can be computed:

$$\begin{aligned} S^{e_1} &= R_1^{-1} \cdot Z_1 \bmod N, \\ S^{e_2} &= R_2^{-1} \cdot Z_2 \bmod N. \end{aligned}$$

If e_1 and e_2 are relatively prime, the group secret key S can be revealed by the Euclidean algorithm.

3.3 The Extension Scheme

In this subsection, the (t, n) threshold untraceable signature scheme will be further extended so that it has the property that the original signers have the ability to prove that they are the true signers. The Partial Signature Generation Phase and the Group Signature Verification Phase will be slightly modified to achieve this purpose as follows.

In the Partial Signature Generation Phase, each user i chooses random integers r_i and \bar{r}_i between 1 and $N - 1$ and computes values $u_i = r_i^L \bmod N$ and $\bar{u}_i = \bar{r}_i^L \bmod N$. u_i and \bar{u}_i are broadcast to all users in B . Once all u_i 's and \bar{u}_i , $s, i \in B$, are available, user i computes the product U , a new value O , and a hash value e as

$$\begin{aligned} U &= \prod_{i \in B} u_i \bmod N = R^L \bmod N, \\ O &= g(\bar{u}_1, \bar{u}_2, \dots, \bar{u}_t), \\ e &= g(U, O, M), \end{aligned}$$

where $R = \prod_{i \in B} r_i \pmod N$.

The partial signature z_i can then be generated by user i :

$$z_i = r_i \cdot K_i^{\prod_{j \in A} (x_i - x_j) \prod_{j \in B, j \neq i} (0 - x_j) \cdot e} \pmod N.$$

In the Group Signature Generation Phase, Z can be calculated by

$$Z = \prod_{i \in B} z_i \pmod N,$$

and $\{e, Z, O\}$ is the group signature of M .

To verify the validity of the group signature $\{e, Z, O\}$, the verifier computes a value U as follows:

$$U = Z^L \cdot Y^e \pmod N.$$

Then, the verifier checks

$$e \stackrel{?}{=} g(U, O, M).$$

If the above equation holds, then the group signature $\{e, Z, O\}$ on the message M is valid.

If the original signers consent to expose their identities, they can show (\bar{r}_i, \bar{u}_i) 's, $i \in B$, to an arbiter. The arbiter checks the following equations:

$$O \stackrel{?}{=} g(\bar{u}_1, \bar{u}_2, \dots, \bar{u}_t), \text{ and}$$

$$\bar{u}_i \stackrel{?}{=} \bar{r}_i^L \pmod N, i \in B.$$

If the above equations hold, the arbiter will believe that these users are the original signers.

With the new value O in the group signature, it is helpless for the verifier to identify the original signers. Therefore, the extension scheme is also untraceable. On the other hand, an arbitrary authorized signing set $B' (\neq B)$ would not be able to show that they are the original signers. This is because they cannot derive \bar{r}_i 's from \bar{u}_i 's unless the RSA scheme is breakable. Furthermore, since $g()$ is a collision free one way hash function, it is infeasible for B' to find t integers \hat{r}_i 's and the corresponding \bar{u}_i 's, $\hat{u}_i = \hat{r}_i^L \pmod N$, such that $O = g(\hat{u}_1, \hat{u}_2, \dots, \hat{u}_t)$.

4. CONCLUSIONS

Desmedt and Frankel proposed the idea of threshold signatures. This paper has classified the threshold signature schemes into threshold traceable and untraceable signature schemes. A threshold untraceable signature scheme has been proposed. We have shown

both the correctness and untraceability of the scheme. However, the proposed scheme indeed needs the assistance of a trusted SDC. It will be very challenging to devise a scheme which does not need the assistance of a trusted center.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous referees for their valuable comments. This work was supported in part by the National Science Council of the Republic of China under contract number NSC88-2213-E218-001.

REFERENCES

1. B. Blakley and G. R. Blakley, "Security of number theoretic public key cryptosystems against random attack," *Cryptologia*, 1978, in three parts: Part 1: Vol. 2, No. 4, 1978, pp.305-321; Part 2: Vol. 3, No. 1, 1979, pp. 29-42; Part 3: Vol. 3, No. 2, 1979, pp. 105-118.
2. G. R. Blakley and I. Borosh, "RSA public key cryptosystems do not always conceal messages," *Computers & Mathematics with Applications*, Vol. 5, No. 3, 1979, pp. 169-178.
3. Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," in *Proceedings of Advances in Cryptology – Crypto '91*, 1991, pp. 457-469.
4. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information, IT-31*, 1985, pp. 469-472.
5. A. Fiat and A. Shamir, "How to prove yourself: Practical solution to identification and signature problems," in *Proceedings of Advances in Cryptology – Crypto '86*, 1987, pp. 186-199.
6. L. C. Guillou and J. J. Quisquater, "A 'Paradoxical' identity-based signature scheme resulting from zero-knowledge," in *Proceedings of Advances in Cryptology – Crypto '88*, 1989, pp. 216-231.
7. L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multisignature," *IEE Proceedings on Computer Digital Technology*, Vol. 141, No. 5, 1994, pp. 307-313.
8. T. Hardjono and Y. Zheng, "A practical digital multisignature scheme based on discrete logarithms," in *Proceedings of Advances in Cryptology – AusCrypt '92*, 1992, pp. 3.16-3.21.
9. C. Li, T. Hwang, and N. Lee, "Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders," in *Proceedings of Advances in Cryptology – EuroCrypto '94*, 1994, pp. 194-204.
10. K. Ohta and T. Okamoto, "A modification of the Fiat-Shamir scheme," in *Proceedings of Advances in Cryptology – Crypto '88*, 1988, pp. 232-243.
11. K. Ohta and T. Okamoto, "A digital multi-signature scheme based on the Fiat-Shamir scheme," in *Proceedings of Advances in Cryptology – AsiaCrypt '91*, 1991, pp. 75-79.
12. T. Okamoto, "A digital multisignature scheme using bijective public-key cryptosystems," *ACM Transactions on Computer Systems*, Vol. 6, No. 8, 1988, pp. 432-441.

13. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem," *Communications of ACM*, Vol. 21, No. 2, 1978, pp. 120-126.
14. A. Shamir, "How to share a secret," *Communications of ACM*, Vol. 22, 1979, pp. 612-613.
15. Y. Zheng, T. Matsumoto, and H. Imai, "Structural properties of one - way hash functions," in *Proceedings of Advances in Cryptology - Crypto '90*, 1990, pp. 285-302.
16. M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptol*, Vol. 1, No. 2, 1988, pp.133-138.
17. E. F. Brickell and D. R. Stinson, "The detection of cheaters in threshold schemes," in *Proceedings of Advances in Cryptology - Crypto '88*, 1990, pp. 564-577.
18. H. Lin and L. Harn, "Fair construction of a secret," *Information Processing Letters*, Vol. 55, No. 1, 1994, pp. 45-47.
19. T. C. Wu and T. S. Wu, "Cheating detection and cheater identification in secret sharing schemes," *IEE Proceedings of Computer Digital Technology*, Vol. 142, No. 5, 1995, pp. 367-369.

Narn-Yih Lee (李南逸) was born in Chiayi, Taiwan, in 1967. He received the B.S. degree in Information Science from Tunghsi University in 1990, the M.S. degree in Applied Mathematics from Chung-Hsing University in 1992 and the Ph.D. degree in Information Engineering from National Cheng-Kung University, Taiwan in 1996. He is currently an associate professor in the Department of Applied Foreign Language, Nan-Tai Institute of Technology, Tainan, Taiwan.

Tzonelih Hwang (黃宗立) is currently a professor in the Institute of Information Engineering, National Cheng-Kung University, Tainan, Taiwan. His research interests include coding theory, cryptography and network security. He is a member of IEEE and IACR (International Association for Cryptologic Research).

Chuan-Ming Li (李泉明) was born in Tainan, Taiwan, R.O.C., in 1964. He received the M.S. degree from the Institute of Information Engineering, National Cheng Kung University. His research interests include data security and cryptography.