Threshold Untraceable Signature for Group Communications*

Chou-Chen Yang[†] Ting-Yi Chang[‡] Min-Shiang Hwang[§]

Department and Graduate Institute of
Computer Science and Information Engineering[†]
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: ccyang@cyut.edu.tw

Department of Computer and Information Science[‡]
National Chiao Tung University
1001 Ta Hsueh Road,
Hsinchu, Taiwan, R.O.C.

Department of Management Information Systems[§]
National Chung Hsing University
250 Kuo Kuang Road,
402 Taichung, Taiwan, R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23742337

July 3, 2003

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-004.

Threshold Untraceable Signature for Group Communications

Abstract

Lee et al. have proposed an untraceable (t, n) threshold signature scheme which can be extended to give the original signers the ability to prove they are the true signers. In this paper, we shall add the requirement of (k, l) threshold-shared verification to Lee et al.'s scheme. In our scheme, any t participants can represent a group to sign messages with/without anonymity, and k verifiers can represent another group to authenticate the signature.

Keywords: Cryptography, digital signature, threshold signature, security, threshold cryptosystem.

1 Introduction

Since digital signature techniques can achieve some tasks such as identifying senders, authenticating message contents, preventing denial of message ownership and protecting ownership, they are playing a more and more important role in our modern electronic society. Traditional digital signatures such as RSA [2, 3, 9, 21] and DSA [8, 19] only allow a single signer to sign a message, and anyone can verify the signature at anytime. For distributing the power of a single signing, the threshold signatures are motivated by the need that arises in organizations to have a group of employees who agree on a message before signing.

In the threshold signature schemes, it is necessary to predetermine the threshold value t so that at least t participants in the group can collaborate to generate a valid signature on behalf of the group, bur only $t - 1$ or fewer participants will not be enough. Anyone who plays the role of a verifier can use the group's public key to authenticate the signature.

In 1991, Desmedt and Frankel [4] proposed a (t, n) threshold signature scheme based on the RSA cryptosystem [21]. Later, Li et al. [14] pointed out that t or more malicious participants can forge the signature without taking any responsibility. In 1994, Harn [5] proposed an alternative (t, n) threshold signature scheme based on Shamir's perfect secret scheme [22] and the modified ElGamal signature [1]. Based on the property of Lagrange polynomials, the group's secret key is distributed into n different shadows to each participant. Any t or more participants can use their shadows to generate individual signatures and combine t individual signatures to obtain threshold signature. On the other hand, in order to trace back to find the original signers in case of a forged document, several (t, n) threshold schemes of traceability [13, 15, 18] and their comments [16, 23, 26] have been proposed.

In 2000, Wang et al. [25] proposed a new (t, n) threshold signature scheme with (k, l) threshold-shared verification. According to the security level of a document, not only the document can be signed by some specified signers in the group (signing group), but also it can be verified by some specified verifiers in another group (verifying group). For example, there are two companies connected in business with each other. The power of signing is distributed for several managers to represent a company to sign a contract with the other company via computer network. The signature of the contract is generated as a threshold signature. For the same reason, the power of verifying is also distributed for several managers to represent the other company to verify the signature of contract.

Unfortunately, Tseng et al. [24] and Hsu et al. [6] separately showed that Wang et al.'s scheme is insecure; any adversary can compute group secret keys from two valid threshold signatures. They also separately proposed their own improved schemes to withstand the attack. Recently, Lee [11] pointed out the signing group secret key of Tseng et al.'s improved scheme is also apt to be disclosed. Fundamentally, the improved scheme [6] has the weaknesses: t or more malicious participants can actually use the Lagrange polynomial formula to derive other participants' secret keys and system secrets. Furthermore, a shared distribution center must take part in the generation of each threshold signature to distribute fresh shadows to all participants, which does not seem to fit in practical applications.

In 2000, Lee et al. [12] proposed an untraceable (t, n) threshold signature scheme based on the Ohta-Okamoto signature scheme [20]. For the sake of privacy and safety, the identities of the signers should be anonymous in a democratic society. At the same time, their scheme can be extended to give the original signers the ability to prove they are true signers, and any t or more malicious participants cannot reconstruct the polynomial to derive other participants' secret keys and system secrets. Furthermore, Lee et al. [12] pointed out that the scheme in [5] can be seen as an untraceable (t, n) threshold signature scheme if the scheme does not provide an individual signature verification mechanism.

In this paper, we will attempt to combine Lee et al.'s (t, n) untraceable scheme and the requirement of (k, l) threshold-shared verification. Moreover, our scheme can be easily modified to provide the individual signatures verification mechanism.

The remainder of our paper is organized as follows. In Section 2, we shall briefly review Lee et al.'s scheme. In Section 3, we shall add the requirement of (k, l) threshold-shared verification to their scheme. In Section 4, we shall analyze the security of our scheme. Finally, in Section 5, we shall give a brief conclusion.

2 Review of Lee et al.'s scheme

In this section, we shall first review Lee et al.'s untraceable (t, n) threshold signature scheme. There is a shared distribution center (SDC for short) which is responsible for initializing the system and generating the parameters in the system. The notation G_s ($|G_s| = n$) is defined as the signing group of n signers and $g_s(|g_s| = t \leq n)$ as any subset of t signers in G_s. The scheme is divided into three phases as follows:

(1) Parameters Generating Phase:

In this phase, SDC is responsible for initializing the system and generating parameters as follows:

1. Randomly choose two large secret primes p and q, and compute a public number $N = p \cdot q$. To ensure that p and q are strong primes, let $p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are also secret primes.

2. Let $\lambda(N) = 2p'q'$ ($\lambda(N)$ is the Carmichael function) be secret and randomly choose a public number $W \approx 10^{50}$, where $gcd(\lambda(N), W) = 1$.

3. Randomly choose a secret primitive α in both $GF(p)$ and $GF(q)$.

4. Randomly choose a secret polynomial $f_s(x) \bmod \lambda(N)$ of degree $t - 1$, where $f_s(0) = d$ and $gcd(\lambda(N), d) = 1$.

5. Compute $S = \alpha^d \bmod N$ as a G_s's secret key and the associated $Y = \alpha^{-d \cdot W} \bmod N$ as this G_s's public key.

6. Randomly select n public and odd integers x_{si} with even $f_s(x_{si})$ [4] for each participant P_{si} in G_s ($i \in G_s$), and their secret keys K_{si} are as follows:

$$K_{si} = \alpha^{s_i} \bmod N, \text{where } s_i = \frac{f_s(x_{si})/2}{[\prod_{\substack{j \in G_s \\ j \neq i}} (x_{si} - x_{sj})]/2} \bmod p'q'. \qquad (1)$$

7. Select a public collision-free one-way hash function $H(\cdot)$.

(2) Individual Signature Generating Phase:

In this phase, P_{si} generates her/his individual signature. Without loss of generality, assume that t participants $P_{s1}, P_{s2}, \cdots, P_{st}$ in g_s are to sign a message m. Each P_{si} randomly chooses an integer r_{si} with $0 < r_{si} < N$, and computes u_{si} as follows:

$$u_{si} = r_{si}^W \bmod N. \tag{2}$$

Then, P_{si} broadcasts u_{si} to the other $t-1$ participants in g_s. Once each P_{si} receives u_j $(j = 1, 2, \cdots, t$ and $j \neq i)$, she/he computes U_s and a hash value e as follows:

$$U_s = \prod_{i \in g_s} u_{si} \bmod N. \tag{3}$$

$$e = H(U_s, m). \tag{4}$$

Then, each P_{si} uses her/his secret key K_{si} to generate her/his individual signature as follows:

$$z_{si} = r_{si} \cdot K_{si}^{\prod_{\substack{j \in G_s \\ j \notin g_s}} (x_{si} - x_{sj}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} (0 - x_{sj}) \cdot e} \bmod N. \tag{5}$$

Each P_{si} sends (z_{si}, m) to a designated clerk who is responsible for the computation of the threshold signature. There is no secret value kept by the clerk, so the clerk can be a general computer.

(3) Threshold Signature Generating and Verifying Phase:

After receiving t individual signatures, the clerk computes the threshold signature as follows:

$$Z_s = \prod_{i \in g_s} z_{si} \bmod N. \tag{6}$$

To verify the threshold signature $\{e, Z_s\}$ for the message m, the verifier first computes a value $\widetilde{U_s}$ as follows:

$$\widetilde{U_s} = Z_s^W \cdot Y^e \bmod N. \tag{7}$$

Then, the verifier checks the following equation:

$$e \stackrel{?}{=} H(\widetilde{U_s}, m). \tag{8}$$

If Equation (8) holds, the threshold signature $\{e, Z_s\}$ is valid.

3 The Proposed Scheme

In this section, we shall add the requirement of (k, l) threshold-shared verification to Lee et al.'s scheme. The notation G_v $(|G_v = l|)$ is defined as the verifying group of l verifiers and $g_v(|g_v| = k \leq l)$ as any subset of k verifiers in G_v. Here, we first present the properties of an untraceable (t, n) threshold signature scheme with (k, l) threshold-shared verification.

- Only t out of n in G_s can generate the signature on behalf of the group.
- Only k out of l in G_v can verify the threshold signature on behalf of the group.
- The signer of the threshold signature cannot be traced.

Our scheme also consists of three phases as follows:

(1) Parameters Generating Phase:

The system notations (SDC, G_s, g_s) and parameters (p, q, p', q', N, W, $\lambda(N)$, α, d, S, Y, x_{si}, K_{si}, $H(\cdot)$) are the same as those in Lee et al.'s scheme. SDC performs the following steps to initialize the system and generate parameters as follows:

1. Randomly choose two numbers a and b such that the greatest common divisor of a and b is 1. When $gcd(a,b)=1$, there must be exactly two integers c and h that satisfy the equation $a\cdot c+b\cdot h=1$. The Extended Euclidean algorithm [17] can find such integers .

2. Randomly choose two secret polynomials $f_s(x) \bmod \lambda(N)$ of degree $t-1$ and $f_v(x) \bmod \lambda(N)$ of degree $k-1$, where $f_s(0)=d\cdot a\cdot c$, $f_v(0)=d\cdot b\cdot h$ and $gcd(\lambda(N),d)=1$.

3. Randomly select l public and odd integers x_{vi} with even $f_v(x_{vi})$ for each participant P_{vi} in G_v ($i \in G_v$), and their secret keys K_{vi} are as follows:

$$K_{vi}=\alpha^{v_i} \bmod N,\text{where } v_i=\frac{f_v(x_{vi})/2}{[\prod\limits_{\substack{j\in G_v\\ j\neq i}}(x_{vi}-x_{vj})]/2} \bmod p'q' \tag{9}$$

(2) Individual Signature Generating Phase:

The message m and the values (u_{si},U_s,e,z_{si}) are separately computed in Equations (2), (3), (4) and (5), which are the same as those in Lee et al.'s scheme.

In order to trace back to find the original signers of a forged document, our scheme can provide an individual signature verification mechanism. In other words, the individual signatures should be verified by a clerk who is responsible for the verification and computation of the threshold signature. Because the clerk has to verify the individual signatures by using the individual signers' public keys before generating the group signature, the clerk knows who has signed the document and securely record it in a database. In the parameters generating phase, SDC distributes a public key y_{si} for each P_{si} in G_s as follows:

$$y_{si}=\alpha^{-s_i\cdot W} \bmod N,\text{where } s_i=\frac{f_s(x_{si})/2}{[\prod\limits_{\substack{j\in G_s\\ j\neq i}}(x_{si}-x_{sj})]/2} \bmod p'q' \tag{10}$$

In the individual signature-generating phase, each P_{si} produces the values (u_{si}, U_s, e, z_{si}) separately by Equations (2), (3), (4) and (5), and added to them is a hash value e_i as follows:

$$e_i = H(u_{si}, m) \tag{11}$$

After receiving (e, e_i, z_{si}, m), the clerk uses P_{si}'s public key y_{si} to compute a value $\widetilde{u_{si}}$ as follows:

$$\widetilde{u_{si}} = z_{si}^W \cdot y_{si}^{\prod_{\substack{j \in G_s \\ j \notin g_s}} (x_{si} - x_{sj}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} (0 - x_{sj}) \cdot e} \mod N \tag{12}$$

and checks the following equation:

$$e_i \stackrel{?}{=} H(\widetilde{u_{si}}, m) \tag{13}$$

If Equation (13) holds, the individual signature z_{si} on the message m is valid. So the individual signature verifying mechanism is put into the individual signature-generating phase. After t individual signatures are verified, the clerk computes the threshold signature Z_s in Equation (6). The remaining steps in the threshold signature generating and verifying phase are the same as those in Lee et al.'s scheme.

(3) Threshold Signature Generating and Verifying Phase:

The generation of the threshold signature Z_s in Equation (6) back in Lee et al.'s scheme is also present here. Then, the threshold signature $\{e, Z_s\}$ of the message m is transmitted to G_v. To verify the group signature, any k out of the l verifiers in G_v should cooperate to authenticate the validity of the signature. Without loss of generality, assume that there are k participants $P_{v1}, P_{v2}, \cdots, P_{vk}$ in g_v. Each P_{vi} randomly chooses an integer r_{vi} with $0 < r_{vi} < N$ and computes u_{vi} and z_{vi} as follows:

$$u_{vi} = r_{vi}^W \mod N \tag{14}$$

$$z_{vi} = r_{vi} \cdot K_{vi}^{\prod_{\substack{j \in G_v \\ j \notin g_v}} (x_{vi} - x_{vj}) \cdot \prod_{\substack{j \in g_v \\ j \neq i}} (0 - x_{vj}) \cdot e} \mod N \tag{15}$$

Then, each P_{vi} transmits u_{vi} and z_{vi} to a clerk who can be randomly chosen from G_v to compute U_v and Z_v as follows:

$$U_v = \prod_{i \in g_v} u_{vi} \bmod N \tag{16}$$

$$Z_v = \prod_{i \in g_v} z_{vi} \bmod N \tag{17}$$

Afterwards, the threshold signature can be verified by using G_s's public key Y to compute a value $\widetilde{U_s}$ as follows:

$$\widetilde{U_s} = (Z_s \cdot Z_v)^W \cdot (U_v)^{-1} \cdot Y^e \bmod N \tag{18}$$

To authenticate the validity of the thresold signature is to check Equation (8). If Equation (8) holds, the threshold signature $\{e, Z_s\}$ on the message m is valid.

Theorem 3.1 *The proposed scheme is a (t, n) threshold signature scheme with (k, l) threshold-shared verification.*

Proof. According to Equations (2), (3) and (4), we can rewrite the hash value e as follows:

$$e = H(\prod_{i \in g_s} r_{si}^W, m)$$

From Equations (1) and (5), (6) the values z_{si} and Z_s can be derived as follows:

$$\begin{aligned}
z_{si} &= r_{si} \cdot K_{si}^{\prod_{\substack{j \in G_s \\ j \notin g_s}} (x_{si} - x_{sj}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} (0 - x_{sj}) \cdot e} \mod N \\
&= r_{si} \cdot \alpha^{s_i \cdot \prod_{\substack{j \in G_s \\ j \notin g_s}} (x_{si} - x_{sj}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} (0 - x_{sj}) \cdot e} \mod N \\
&= r_{si} \cdot \alpha^{\frac{f_s(x_{si})}{\prod_{\substack{j \in G_s \\ j \neq i}} (x_{si} - x_{sj})} \cdot \prod_{\substack{j \in G_s \\ j \notin g_s}} (x_{si} - x_{sj}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} (0 - x_{sj}) \cdot e} \mod N \\
&= r_{si} \cdot \alpha^{f_s(x_{si}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} \frac{(0 - x_{sj})}{(x_{si} - x_{sj})} \cdot e} \mod N
\end{aligned}$$

and

$$Z_s = \prod_{i \in g_s} r_{si} \cdot \alpha^{\sum_{i \in g_s} f_s(x_{si}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} \frac{(0 - x_{sj})}{(x_{si} - x_{sj})} \cdot e} \mod N$$

By using Lagrange interpolating polynomial, with the knowledge of t pairs of $(x_{si}, f_s(x_{si}))$, the unique $(t-1)$th degree polynomial $f_s(x_{si})$ and $f_s(0)$ can be determined as follows:

$$\begin{aligned} f_s(x) &= \sum_{i \in g_s} f_s(x_{si}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} \frac{(x - x_{sj})}{(x_{si} - x_{sj})} \mod \lambda(N) \\ f_s(0) &= \sum_{i \in g_s} f_s(x_{si}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} \frac{(0 - x_{sj})}{(x_{si} - x_{sj})} \mod \lambda(N) \end{aligned}$$

Thus,

$$\begin{aligned} Z_s &= \prod_{i \in g_s} r_{si} \cdot \alpha^{\sum_{i \in g_s} f_s(x_{si}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} \frac{(0 - x_{sj})}{(x_{si} - x_{sj})} \cdot e} \mod N \\ &= \prod_{i \in g_s} r_{si} \cdot \alpha^{d \cdot a \cdot c \cdot e} \mod N \end{aligned}$$

For the same reason, by using Lagrange interpolating polynomial, the value Z_v can be derived from Equations (9), (15) and (17) as follows:

$$Z_v = \prod_{i \in g_v} r_{vi} \cdot \alpha^{d \cdot b \cdot h \cdot e} \mod N$$

If the threshold signature $\{e, Z_s\}$ is valid and the value Z_v is produced by k verifiers in G_v, the values U_s and $\widetilde{U_s}$, separately computed in Equations (3) and (18), should be as follows:

$$\begin{aligned} U_s &= \prod_{i \in g_s} u_{si} \mod N \\ &= \prod_{i \in g_s} r_{si}^W \mod N \end{aligned}$$

and

$$\widetilde{U_s} = (Z_s \cdot Z_v)^W \cdot (U_v)^{-1} \cdot Y^e \mod N$$

$$
\begin{aligned}
&= (\prod_{i\in g_s} r_{si}\cdot\alpha^{d\cdot a\cdot c\cdot e}\cdot\prod_{i\in g_v} r_{vi}\cdot\alpha^{d\cdot b\cdot h\cdot e})^W\cdot(\prod_{i\in g_v} r_{vi}^W)^{-1}\cdot(\alpha^{-d\cdot W})^e \bmod N\\
&= \prod_{i\in g_s} r_{si}^W\cdot\prod_{i\in g_v} r_{vi}^W\cdot\alpha^{d\cdot e\cdot W\cdot(a\cdot c+b\cdot h)}\cdot\alpha^{-d\cdot W\cdot e}\cdot(\prod_{i\in g_v} r_{vi}^W)^{-1} \bmod N\\
&= \prod_{i\in g_s} r_{si}^W \bmod N
\end{aligned}
$$

Therefore, the correctness of Equation (8) can be verified. In this case, $\{e, Z_s\}$ must be a signature generated by t signers in G_s, and only k verifiers in G_v can verify it. *Q.E.D.*

Theorem 3.2 *The proposed (t, n) threshold signature scheme with (k, l) threshold-shared verification is untraceable.*

Proof. Assume that there are two subsets g_s and g'_s in G_s, where $|g_s| = |g'_s| = t$. Each P_{si} in g_s generates her/his individual signature z_{si} and the threshold signature $\{e, Z_s\}$. If it is impossible to tell who collaborate to generate the threshold signature $\{e, Z_s\}$, our scheme is untraceable. In other words, the pair (r'_{si}, u'_{si}) generated by P'_{si} in g'_s is indistinguishable from (r_{si}, u_{si}) originally generated by P_{si} in g_s. From z_{si} in Equation (5), each P'_{si} in g'_s can compute (r'_{si}, u'_{si}) as follows:

$$
r'_{si} = z_{si}\cdot\left({K'}_{si}^{\prod_{j\in G_s, j\notin g'_s}(x_{si}-x_{sj})\cdot\prod_{j\in g'_s, j\neq i}(0-x_{sj})\cdot e}\right)^{-1} \bmod N
$$

and

$$
u'_{si} = r'^W_{si} \bmod N
$$

Since the threshold signature Z_s can be expressed as:

$$
\begin{aligned}
Z_s &= \prod_{i\in g_s} z_{si} \bmod N\\
&= \prod_{i\in g_s}\left(r_{si}\cdot K_{si}^{\prod_{j\in G_s, j\notin g_s}(x_{si}-x_{sj})\cdot\prod_{j\in g_s, j\neq i}(0-x_{sj})\cdot e}\right) \bmod N
\end{aligned}
$$

$$
\begin{aligned}
&= \prod_{i \in g'_s} \left(r'_{si} \cdot {K'}_{si}^{\prod_{j \in G_s, j \notin g'_s} (x_{si} - x_{sj}) \cdot \prod_{j \in g'_s, j \neq i} (0 - x_{sj}) \cdot e}\right) \bmod N \\
&= \prod_{i \in g_s} r_{si} \cdot \alpha^{d \cdot a \cdot c \cdot e} \bmod N \\
&= \prod_{i \in g'_s} r'_{si} \cdot \alpha^{d \cdot a \cdot c \cdot e} \bmod N
\end{aligned}
$$

It implies that $\prod_{i \in g_s} r_{si} = \prod_{i \in g'_s} r'_{si} \bmod N$, so the equation $\prod_{i \in g_s} u_{si} = \prod_{i \in g'_s} u'_{si} \bmod N$ is also true. *Q.E.D.*

Like Lee et al.'s scheme, our scheme can also be further extended (See [12] for a more detailed description) to give the original signers the ability to prove that they are the true signers. In the individual signature-generating phase, each P_{si} randomly chooses an integer $\overline{r_{si}}$ and computes a value $\overline{u_{si}} = \overline{r_{si}}^L \bmod N$, additionally. Each P_{si} broadcasts $\overline{u_{si}}$ to the other $t-1$ participants in g_s to produce U in Equation (3) and a new hash value E as follows:

$$E = H(\overline{u_{s1}}, \overline{u_{s2}}, \cdots, \overline{u_{st}})$$

Then, each P_{si} in g_s replaces Equation (4) with the following equation:

$$e = H(U_s, E, m)$$

After computing Equations (5) and (6), $\{e, Z_s, E\}$ becomes the threshold signature of m. After performing Equations (18), (17) and (18), the threshold signature can be verified by the following equation in place of Equation (8).

$$e = H(\widetilde{U_s}, E, m)$$

If the above equation holds, the threshold signature $\{e, Z_s, E\}$ on the message m is valid. If the original signers agree to make it public that they are the true signers, they can show $(\overline{r_{si}}, \overline{u_{si}})$ to an arbiter. The arbiter checks the following equations:

$$E \stackrel{?}{=} H(\overline{u_{s1}}, \overline{u_{s2}}, \cdots, \overline{u_{st}})$$

and

$$\overline{u_{si}} \stackrel{?}{=} \overline{r_{si}}^{L} \bmod N$$

If the above equations hold, the arbiter will believe that they are the true signers.

Theorem 3.3 *The individual signatures can be verified by the clerk.*

Proof. The value u_{si} separately computed in Equations (2) and (18

$$u_{si} = r_{si}^{W} \bmod N$$

and

$$\begin{aligned}
u_{si} &= z_{si}^{W} \cdot y_{si}^{\prod\limits_{\substack{j\in G_s\\ j\notin g_s}} (x_{si} - x_{sj}) \cdot \prod\limits_{\substack{j\in g_s\\ j\neq i}} (0 - x_{sj}) \cdot e} \bmod N \\
&= (r_{si} \cdot K_{si}^{\prod\limits_{\substack{j\in G_s\\ j\notin g_s}} (x_{si} - x_{sj}) \cdot \prod\limits_{\substack{j\in g_s\\ j\neq i}} (0 - x_{sj}) \cdot e})^{W} \cdot \\
&\quad y_{si}^{\prod\limits_{\substack{j\in G_s\\ j\notin g_s}} (x_{si} - x_{sj}) \cdot \prod\limits_{\substack{j\in g_s\\ j\neq i}} (0 - x_{sj}) \cdot e} \bmod N \\
&= (r_{si} \cdot \alpha^{s_i \cdot \prod\limits_{\substack{j\in G_s\\ j\notin g_s}} (x_{si} - x_{sj}) \cdot \prod\limits_{\substack{j\in g_s\\ j\neq i}} (0 - x_{sj}) \cdot e})^{W} \cdot \\
&\quad \alpha^{-s_i \cdot W \cdot \prod\limits_{\substack{j\in G_s\\ j\notin g_s}} (x_{si} - x_{sj}) \cdot \prod\limits_{\substack{j\in g_s\\ j\neq i}} (0 - x_{sj}) \cdot e} \bmod N \\
&= r_{si}^{W} \bmod N
\end{aligned}$$

Therefore, the correctness of Equation (13) can be verified. That is, (e, e_i, z_{si}) must be an individual signature on message m. *Q.E.D.*

Obviously, in our scheme, if P_{si} in G_s has computed e_i and sent it to the clerk to verify her/his individual signature, the properties of our scheme are the same as those of the schemes in [6, 24]. In other words, the participants in the signing group can determine whether or not to stay anonymous. Furthermore, SDC can be revoked after the parameters generating phase in our scheme.

4 Security Analysis

The security of our proposed scheme is the same as that of Lee et al.'s scheme, which is based on the difficulty of breaking the RSA scheme [21]. Theorem 1 shows that any subset of t participants in G_s can generate the threshold signature and any subset of k participants in G_v can verify the group signature. Note that the attackers on the proposed schemes may come from inside (denoted as impostors) or outside (denotes as adversary) of the signing/verifying group. In the rest of this section, some possible attacks are raised and fought against to prove the security of our scheme.

Attack 1: An adversary tries to reveal G_s's secret key S from the known information as the following cases:

Case 1: The equation $Y = S^{-W} \bmod N$ and G_s's keys Y, N and the parameter W are known. It is as difficult as breaking the RSA scheme to reveal G_s's secret key S.

Case 2: The equation $S = \alpha^d \bmod N$ is known. The adversary should first reconstruct the polynomial $f_s(x) \bmod \lambda(N)$ to obtain $f_s(0) = d \cdot a \cdot c$. Then, she/he has to calculate the multiplicative inverse for $a \cdot c \bmod \lambda(N)$. However, $f_s(x), \lambda(N), a, c$ and the primitive element α are secret.

Case 3: The equations $Z_s = \prod_{i \in g_s} \cdot S^{a \cdot c \cdot e} \bmod N, U = \prod_{i \in g_s} r_{si}^W \bmod N$ and a valid signature $\{e, Z_s\}$ are known. The adversary should first find out the random product $\prod_{i \in g_s} r_{si}$ from U. Then, she/he has to calculate the $(a \cdot c \cdot e) - th$ root of $Z_s \cdot (\prod_{i \in gs} r_{si})^{-1} \bmod N$. However, retrieving $\prod_{i \in g_s} r_{si}$ from U is as difficult as breaking the RSA scheme, and the difficulty of extracting the $(a \cdot c \cdot e) - th$ root of $Z_s \cdot (\prod_{i \in gs} r_{si})^{-1} \bmod N$ is equivalent to breaking the RSA scheme when $gcd(a \cdot c \cdot e, \lambda(N)) = 1$ and equivalent to factoring N if $gcd(a \cdot c \cdot e, p - 1) = 1$ or $gcd(a \cdot c \cdot e, q - 1) = 1$. Moreover, the parameters (a, c) are secret.

Attack 2: An adversary tries to reveal P_{si}'s secret key K_{si} in G_s from the known information.

Case 1: The equation $y_{si} = K_{si}^{-W} \bmod N$ and P_{si}'s public keys y_{si}, N and the parameter W are known. It is as difficult as breaking the RSA scheme to reveal P_{si}'s secret key K_{si}.

Case 2: The Equation (1) and the public value x_{si} are known. It is infeasible for the adversary to derive P_{si}'s secret key K_{si} if $f_s(x_{si}), \alpha, p'$ and q' are unknown.

Case 3: The Equations (2), (5) and the individual signature z_{si} are known. The adversary should first find out the random number r_{si} from u_{si}. Then, she/he has to calculate the $(\prod_{\substack{j \in G_s \\ j \notin g_s}} (x_{si} - x_{sj}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} (0 - x_{sj}) \cdot e) - th$ root of $z_{si} \cdot r_{si}^{-1} \bmod N$. However, retrieving r_{si} from u_{si} is as difficult as breaking the RSA scheme. The difficulty of extracting the $(\prod_{\substack{j \in G_s \\ j \notin g_s}} (x_{si} - x_{sj}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} (0 - x_{sj}) \cdot e) - th$ root of $z_{si} \cdot r_{si}^{-1} \bmod N$ is equivalent to breaking the RSA scheme.

Attack 3: An adversary tries to reveal P_{vi}'s secret key K_{vi} in G_v from the known information.

As with Cases 1 and 2 in *Attack* 1, the adversary should face the difficulty of breaking the RSA scheme.

Attack 4: An adversary tries to impersonate P_{si} in g_s.

The adversary first chooses a random integer r'_{si} with $0 < r'_{si} < N$, and broadcasts $u_{si} = r'^{W}_{si} \bmod N$. The adversary can obtain the productive value

$U' = \prod_{\substack{j \in g_s \\ j \neq i}} u_{sj} \cdot u_{si} \bmod N$ and the hash value $e' = H(U'_s, m)$. Without knowing P_{si}'s secret key K_{si}, the adversary should face the difficulty of generating a valid value z'_{si} in Equation (18) to satisfy the following equation:

$$z'^{W}_{si} \cdot \prod_{\substack{j \in g_s \\ j \neq i}} z^{W}_{sj} = U'_s \cdot Y^{-e} \cdot Z_v^{-W} \cdot U_v \bmod N$$

Moreover, if the broadcasting cryptosystems [7, 10] or the secret channel exists in G_s, it can keep the adversary from knowing the productive values $\prod_{\substack{j \in g_s \\ j \neq i}} u_{sj} \bmod N$ and $\prod_{\substack{j \in g_s \\ j \neq i}} z^{W}_{sj} \bmod N$.

Attack 5: An adversary tries to impersonate P_{vi} in g_v.
As with *Attack 4*, the adversary should face the difficulty of generating a valid value z'_{vi} in Equation (18).

Attack 6: In G_s, t or more malicious impostors try to reconstruct the secret polynomial $f_s(x)$ of degree $t-1$ to obtain other participants' secret keys K_{si}. Since *SDC* distributes $K_{si} = \alpha^{si} \bmod N$ in place of s_i, t or more pairs (x_{si}, K_{si}) cannot help reconstruct $f_s(x)$. If the impostor tries to reveal s_i from K_{si}, it is as difficult as the problem of solving the discrete logarithm modulo a composite number N if α is known. Furthermore, α and $\lambda(N)$ are secret in our scheme. On the other hand, t or more malicious impostors cannot collude to retrieve $\lambda(N)$.

Attack 7: In G_v, k or more malicious impostors try to reconstruct the secret polynomial $f_k(x)$ of degree $k-1$ to obtain other participants' secret keys K_{vi}. As with *Attack 6*, k or more malicious impostors in G_v cannot reconstruct the secret polynomial of degree $k-1$ to obtain other participants' secret keys K_{vi}.

Attack 8: An adversary tries to forge the group signature $\{e, Z_s\}$ for the message m.

The adversary randomly computes the productive value U_s and the hash value $e = H(U_s, m)$. Then, the adversary has to figure out Z_s from $Z_s^W = U_s \cdot Y^{-e} \cdot Z_v^{-W} \cdot U_v \bmod N$. It is as difficult as breaking the RSA scheme. On the other hand, the adversary may also try to randomly generate a threshold signature $\{e, Z_s\}$ and compute $U_s = (Z_s \cdot Z_v)^W \cdot Y^e \cdot (U_v)^{-1} \bmod N$. However, H is a collision-free one-way hash function; it is difficult to find a message m' such that $e = H(U_s, m')$.

Attack 9: All P_{si} and P_{vi} should separately keep the random values r_{si} and r_{vi} secret.

From two valid threshold signatures $\{e_1, Z_{s1}\}$ and $\{e_2, Z_{s2}\}$, the adversary can obtain the following equations:

$$\begin{cases} S^{e_1} = (\prod_{i \in g_s} r_{si})^{-1} \cdot Z_{s1} \bmod N, \\ S^{e_2} = (\prod_{i \in g_s} r_{si})^{-1} \cdot Z_{s2} \bmod N. \end{cases}$$

$$\begin{cases} (\alpha^{d \cdot b \cdot h})^{e_1} = (\prod_{i \in g_v} r_{vi})^{-1} \cdot Z_{v1} \bmod N, \\ (\alpha^{d \cdot b \cdot h})^{e_2} = (\prod_{i \in g_v} r_{vi})^{-1} \cdot Z_{v2} \bmod N. \end{cases}$$

If $gcd(e_1, e_2) = 1$, the group secret key S and the value $\alpha^{d \cdot b \cdot h}$ can be revealed by the Euclidean algorithm. Then, anyone can easily use S and $\alpha^{d \cdot b \cdot h}$ to generate and verify other threshold signatures without cooperation, respectively.

5 Conclusion

In this paper, we have added the requirement of (k, l) threshold-shared verification to Lee et al.'s scheme by using the Extended Euclidean algorithm and demonstrated the ability of our new scheme to work against some possible attacks. Our security analysis has revealed that our scheme can withstand these attacks under factorization. Moreover, our scheme provides both traceability mode and untraceability mode for the participants to choose from. With untraceability, the original signers also have the ability to prove they are the true signers.

References

[1] G. B. Agnew, B. C. Mullin, and S.A. Vanstone, "Improved digital signature scheme based on discrete exponentiation," *Electronics Letters*, vol. 26, no. 14, pp. 1024–1025, 1990.

[2] C. C. Chang and M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *IEE Electronics Letters*, vol. 32, no. 15, pp. 1365–1366, 1996.

[3] S. W. Changchien, M. S. Hwang, and K. F. Hwang, "A batch verifying and detecting multiple RSA digital signatures," *International Journal of Computational and Numerical Analysis and Applications*, vol. 2, no. 3, pp. 303–307, 2002.

[4] Y. Desmedt and Y. Frankel, "Shared generation of authenticators," in *Advances in Cryptology, CRYPTO'91*, pp. 457–469, 1991.

[5] L. Harn, "Group-oriented *(t, n)* threshold signature and digital multisignature," *IEE Proceedings - Computers and Digital Techniques*, vol. 141, no. 5, pp. 307–313, 1994.

[6] C. L. Hsu, T. S. Wu, and T. C. Wu, "Improvements of threshold signature and authenticated encryption for group communications," *Information Processing Letters*, vol. 81, no. 1, pp. 41–45, 2002.

[7] M. S. Hwang, C. C. Lee, and T. Y. Chang, "Broadcasting cryptosystem in computer networks using geometric properties of lines," *Journal of Information Science and Engineering*, vol. 18, no. 3, pp. 373–378, 2002.

[8] M. S. Hwang, C. C. Lee, and Y. C. Lai, "Traceability on low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals on Electronics, Communications and Computer Sciences*, vol. E85-A, no. 5, pp. 1181–1182, 2002.

[9] M. S. Hwang, I. C. Lin, and K. F. Hwang, "Cryptanalysis of the batch verifying multiple RSA digital signatures," *Informatica*, vol. 11, no. 1, pp. 15–19, 2000.

[10] C. C. Lee, T. Y. Chang, and M. S. Hwang, "A simple broadcasting cryptosystem in computer networks using exclusive-or," *to appear in International Journal of Computer Applications in Technology*, 2003.

[11] N. Y. Lee, "The security of the improvement on the generalization of threshold signature and authenticated encryption," *IEICE Transactions on Fundamentals*, vol. E85-A, no. 10, pp. 2364–2367, 2002.

[12] N. Y. Lee, T. Hwang, and C. M. Li, "*(t, n)* threshold untraceable signatures," *Journal of Information Science and Engineering*, vol. 16, no. 6, pp. 835–845, 2000.

[13] W. B. Lee and C. C. Chang, "*(t, n)* threshold digital signature with traceability property," *Journal of Information Science and Engineering*, vol. 15, no. 5, pp. 669–678, 1999.

[14] C. M. Li, T. Hwang, and N. Y. Lee, "Remark on the threshold rsa signature scheme," in *Advances in Cryptology, CRYPTO'93*, pp. 413–420, 1994.

[15] C. M. Li, T. Hwang, and N. Y. Lee, "Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders," in *Advances in Cryptology, Eurocrypt'94*, pp. 194–204, 1994.

[16] Z. C. Li, L. C. K. Hui, K. P. Chow, C. F. Chong, W. W. Tsang, and H. W. Chan, "Security of wang et al.'s group-oriented *(t, n)* threshold signature schemes with traceable signers," *Information Processing Letters*, vol. 80, no. 6, pp. 295–298, 2001.

[17] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography.* CRC Press, 1996.

[18] M. Michels and P. Horster, "On the risk of disruption in several multiparty signature schemes," in *Asiacrypt'96*, pp. 334–345, 1996.

[19] National Institute of Satndards and Technology (NIST), "The digital sinature standard proposed by NIST," *Communications of the ACM*, vol. 35, no. 7, pp. 36–40, 1992.

[20] K. Ohta and T. Okamoto, "A modification of the Fiat-Shamir scheme," *Crypto'88*, pp. 232–243, 1988.

[21] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[22] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.

[23] Y. M. Tseng and J. K. Jan, "Attacks on threshold signature schemes with traceable signers," *Information Processing Letters*, vol. 71, no. 1, pp. 1–4, 1999.

[24] Y. M. Tseng, J. K. Jan, and H. Y. Chien, "On the security of generalization of threshold signature and authenticated encryption," *IEICE Transactions on Fundamentals*, vol. E84-A, no. 10, pp. 2606–2609, 2001.

[25] C. T. Wang, C. C. Chang, and C. H. Lin, "Generalization of threshold signature and authenticated encryption for group communications," *IEICE Transactions on Fundamentals*, vol. E83-A, no. 6, pp. 1228–1237, 2000.

[26] C. T. Wang, C. H. Lin, and C. C. Chang, "Research note threshold signature schemes with traceable signers in group communications," *Computer Communications*, vol. 21, no. 8, pp. 771–776, 1998.