Journal of Zhejiang University SCIENCE
ISSN 1009-3095
http://www.zju.edu.cn/jzus
E-mail: jzus@zju.edu.cn

Applying two channels to vector space secret sharing based multi-signature scheme

XIAO Qing-hua (肖清华)†, PING Ling-di (平玲娣), CHEN Xiao-ping (陈小平), PAN Xue-zeng (潘雪增)

(*School of Computer Science, Zhejiang University, Hangzhou 310027, China*)

†E-mail: foxqinghua@etang.com

Received Jan. 20, 2004; revision accepted Oct. 29, 2004

Abstract: Secret sharing and digital signature is an important research area in information security and has wide applications in such fields as safeguarding and legal use of confidential information, secure multiparty computation and electronic commerce. But up to now, study of signature based on general vector space secret sharing is very weak. Aiming at this drawback, the authors did some research on vector space secret sharing against cheaters, and proposed an efficient but secure vector space secret sharing based multi-signature scheme, which is implemented in two channels. In this scheme, the group signature can be easily produced if an authorized subset of participants pool their secret shadows and it is impossible for them to generate a group signature if an unauthorized subset of participants pool their secret shadows. The validity of the group signature can be verified by means of verification equations. A group signature of authorized subset of participants cannot be impersonated by any other set of participants. Moreover, the suspected forgery can be traced, and the malicious participants can be detected in the scheme. None of several possible attacks can successfully break this scheme.

Key words: Vector space secret sharing, Multi-signature, Discrete logarithm, Chinese remainder theorem
doi:10.1631/jzus.2005.A0056 **Document code:** A **CLC number:** TP309

INTRODUCTION

Digital signatures play an important role in our modern electronic society because they have the properties of integrity and authentication. The integrity property ensures that the received message is not modified, and the authentication property ensures that the sender is not impersonated. In well-known conventional digital signatures, such as RSA and DSA, a single signer is sufficient to produce a valid signature, and anyone can verify the validity of any given signature. However, on many occasions, we need to share the responsibility of the signing message with a set of signers. Issuing checks for a company is an example for this. For the sake of security, it may be a policy of a company that checks must be signed by a group of individuals rather than one person. Secret sharing signature schemes (Gennaro *et al*., 1996; Safavi *et al.*, 1999) and multi-signature schemes (Harn and Kiesler, 1989; Okamoto, 1988; Harn, 1994b) are designed to solve such problems. There are two major differences between secret sharing signature and multi-signature schemes. Firstly, it is not necessary to restrict the number of signers to generate a valid signature in a multi-signature scheme. In contrast to a multi-signature scheme, a so-called threshold value must be predetermined to guarantee the security of the system in a secret sharing signature scheme. Secondly, a secret sharing signature represents the signature signed by the group while a multi-signature is a signature that represents a set of individuals who sign the message. Consequently, a secret sharing signature is suitable for the case where the members of a group are allowed to sign on behalf of the group.

But when cheaters appear in signatures, and if we want to detect and trace them, we may need to combine these two signatures to form a new one. We call it secret sharing based multi-signature scheme (Desmedt and Frankel, 1992b).

RELATED WORKS

Since the secret sharing based multi-signature scheme can solve problems that cannot be solved by secret sharing signature and multi-signature scheme individually, much research had been focused on the topic. Desmedt and Frankel (1992b) applied a trusted key authentication center to determine the group's secret key and the secret keys of all group members. However, Li *et al.*(1994) pointed out that Desmedt and Frankel's scheme may suffer from conspiracy attacks and that the secret keys can be revealed if t or more participants act in collusion. To avoid conspiracy attacks, the new proposed schemes (Li *et al.*, 1995) attach a random number to the secret key held by each member, so that the security of their schemes is guaranteed. Similarly, Harn (1994a) used the cryptographic technique of Shamir's perfect secret sharing which is based on the Lagrange interpolating polynomial and digital signature algorithm to construct a (t, n) threshold signature scheme designed to partition the group's secret key into n different shadows. By collecting any of the t shadows, the group signature can be easily generated. Michels and Horster (1996) showed that these solutions mentioned above are all vulnerable to forgery attack by an inside attacker and cannot withstand conspiracy attacks. Desmedt and Frankel (1992a) presented another threshold signature scheme based on RSA. But similar to their previous solution (Desmedt and Frankel, 1992b), the secret keys can still be revealed by conspiracy attacks.

Most of the researches above consider only threshold structures: the system tolerates the presence of less than t corrupted players, and the subsets of players who can sign a message are those with k or more players. To thwart this weakness, Brickell (1989) introduced vector space construction that is more general than the threshold structure. In order to improve the security of vector space secret sharing, Padró and Sáez (1999) proposed a solution that can efficiently find out whether some cheaters exist. However, this solution cannot reveal the cheaters' identities. Xu *et al.*(2002) improved Padró's scheme and presented another secure vector space secret sharing scheme.

Recently, in order to make the signature scheme more practical and general, Herranz *et al.*(2003) extended the vector space structure to a so-called general access structure and proposed a framework allowing a general access structure of players to sign and a general family of dishonest players that the scheme can tolerate. Using general access structure, Ventzislav *et al.*(2001) also built some unconditionally secure proactive secret sharing schemes. But up to now, study of signature based on vector space and general access structure is still very weak.

Almost all of the signature schemes mentioned above are implemented in one channel. The main contribution of this paper is to design a two-channel secure vector space traceable multi-signature scheme. Security of the signature scheme in each channel is equal to that of an independent one. Malicious users can forge the signature only if the signatures in both channels can be forged. In our designed scheme, when a faulty signature is presented, cheaters can be detected and traced easily. In terms of performance, this scheme should not be less efficient than most of solutions available (e.g., Li *et al*., 1995; Harn, 1994a; Desmedt and Frankel, 1992a). We organize the rest of the paper as follows. First of all, secure vector space secret sharing scheme is reviewed and analyzed. Then we present our new proposed scheme and analyze its security and efficiency, respectively. At last, we draw our conclusions.

SECURE VECTOR SPACE SECRET SHARING

This section contains some background and formal definitions of vector space secret sharing scheme (Brickell, 1989; Stinson, 1995), which will be referred in the rest of this paper.

Let T be an access structure on a set of participants $P=\{p_1, p_2, \ldots, p_n\}$ and $D\notin P$ a special participant called the dealer. T is said to be a vector space access structure if, for some vector space $\boldsymbol{E}=K^r$ over a finite field K, there exists a function

$$\psi: P\cup\{D\}\rightarrow\boldsymbol{E} \tag{1}$$

such that $A\in T$ if and only if the vector $\psi(D)$ can be expressed as a linear combination of the vectors in the set $\psi(A)=\{\psi(p_i)|p_i\in A\}$. If T is a vector space access structure, we can construct an ideal secret sharing scheme for T with set of secrets K: given a secret

value $k \in K$, the dealer takes a random $\boldsymbol{v} \in \boldsymbol{E}$, such that

$$k = \boldsymbol{v} \cdot \psi(D) \tag{2}$$

and sends to the participant $p_i \in P$ his share

$$s_{p_i} = \boldsymbol{v} \cdot \psi(p_i) \in K \tag{3}$$

A scheme constructed in this way is called a vector space secret sharing scheme. Let $A \in T$ be an authorized subset, then we have:

$$\psi(D) = \lambda_1 \psi(p_1) + \lambda_2 \psi(p_2) + \cdots + \lambda_l \psi(p_l),$$

for some $\lambda_i \in K$. In order to recover the secret, the players of A compute $\lambda_1 s_{p_1} + \lambda_2 s_{p_2} + \cdots + \lambda_l s_{p_l} = k$.

Unfortunately, such scheme is open to the Tompa-Woll attack (Tompa and Woll, 1988). To ensure the security of vector space secret sharing, Padró and Sáez (1999) proposed an improved scheme. The dealer D selects a vector pair ($\boldsymbol{v}_1$, $\boldsymbol{v}_2$), such that: $\boldsymbol{v}_1 = (k, v_{21}, \cdots, v_{r1})$, $\boldsymbol{v}_2 = (k^2, v_{22}, \cdots, v_{r2})$, $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \boldsymbol{E}$. D computes $s_{p_{i1}} = \boldsymbol{v}_1 \cdot \psi(p_i)$, $s_{p_{i2}} = \boldsymbol{v}_2 \cdot \psi(p_i)$ ($1 \le i \le n$), and delivers $(s_{p_{i1}}, s_{p_{i2}})$ to each p_i, i=1, 2, …, n. When is necessary to recover k, all the members in A show their shadows pair $(s_{p_{i1}}, s_{p_{i2}})$, and compute $k_1 = \lambda_1 s_{p_{11}} + \lambda_2 s_{p_{21}} + \cdots + \lambda_l s_{p_{l1}}$, $k_2 = \lambda_1 s_{p_{12}} + \lambda_2 s_{p_{22}} + \cdots + \lambda_l s_{p_{l2}}$. If the equation $k_2 = k_1^2$ holds, the recovered secret k_1 is valid. Otherwise, it denotes some participants in A may not be honest.

PROPOSED SCHEME

We assume that there is an honest dealer D to determine the secret and to deliver the secret shadows to all the participants. The word "honest" implies that the dealer must ensure that the secret information is not disclosed or revealed to unauthorized people and prevent unauthorized modification or destruction of data. It is expected that if the dealer is compromised, the security of the whole system will be lost.

Let us divide our scheme into three phases: the system initialization phase, the partial signature generation and verification phase, the group signature generation and verification phase.

System initialization phase

The honest dealer D selects the following parameters: (1) A huge prime N, $2^{511} < N < 2^{512}$ and a generator g with order N' in $GF(N)$, where $N' = pq$, $N' | (N-1)$, p and q are two large primes, and $2^{160} < p, q < 2^{161}$; (2) A one-way hash function $h()$; (3) Parameters σ_p, σ_q, where

$$\begin{aligned} \sigma_p &= 1 \bmod p = 0 \bmod q \\ \sigma_q &= 0 \bmod p = 1 \bmod q \end{aligned} \tag{4}$$

Additionally, suppose $A = \{p_1, p_2, \ldots, p_l\}$ is the subset authorized to sign a message. We can refer other parameters mentioned before, among which $\lambda_i \in K$ can be computed by any participants. D computes the group public key $Y = g^{k_1} \bmod N$, delivers $(s_{p_{i1}}, s_{p_{i2}})$ to each p_i, i=1, 2, …, n, and publishes N, N', σ_p, σ_q, g, h, Y, ψ and keeps k_1, $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ in secret.

Distribution of secret shadows and verification phase

Each participant p_i in A has to generate a partial signature for message m as follows. p_i picks two random numbers $b_{ip} \in [1, p-1]$, $b_{iq} \in [1, q-1]$ and computes his public key pair (y_{i1}, y_{i2}) as $y_{i1} = g^{s_{p_{i1}}} \bmod N$, $y_{i2} = g^{s_{p_{i2}}} \bmod N$, b_i as

$$b_i = \sigma_p b_{ip} + \sigma_q b_{iq} \bmod N' \tag{5}$$

and r_i as

$$r_i = g^{b_i} \bmod N \tag{6}$$

It is worth noting here that the public keys of each participant are also regarded as his identity information. Each p_i makes r_i publicly available through a broadcast channel. Once all r_i are available, each p_i can compute

$$R = \prod_{p_i \in A} r_i \bmod N \tag{7}$$

$$HASH = h(m, R, A) \tag{8}$$

Then p_i uses his secret shadows and the random number b_i to compute

$$s_i = s_{p_{i1}} \lambda_i + b_{ip} HASH \bmod p = s_{p_{i2}} + b_{iq} HASH \bmod q \tag{9}$$

p_i sends the partial signature $\{m, r_i, s_i\}$ to a designated clerk responsible for collecting the partial signatures and producing the group signature. Since no secret information is kept, the clerk can be anyone in the system. The clerk can check whether the equation

$$g^{s_i} = (y_{i1})^{\lambda_i \sigma_p} r_i^{HASH} y_{i2}^{\sigma_q} \bmod N \tag{10}$$

holds. If so, the partial signature from p_i is valid. The correctness of this equation can be easily seen as follows.

Since

$$s_i = s_{p_{i1}} \lambda_i + b_{ip} HASH \bmod p = s_{p_{i2}} + b_{iq} HASH \bmod q,$$

we have

$$s_i = (s_{p_{i1}} \lambda_i + b_{ip} HASH)\sigma_p + (s_{p_{i2}} + b_{iq} HASH)\sigma_q \bmod N'$$

$$g^{s_i} = g^{(s_{p_{i1}} \lambda_i + b_{ip} HASH)\sigma_p + (s_{p_{i2}} + b_{iq} HASH)\sigma_q \bmod N'} \bmod N$$

$$= g^{s_{p_{i1}} \lambda_i \sigma_p} g^{(b_{ip}\sigma_p + b_{iq}\sigma_q) HASH} g^{s_{p_{i2}} \sigma_q} \bmod N$$

$$= (y_{i1})^{\lambda_i \sigma_p} r_i^{HASH} y_{i2}^{\sigma_q} \bmod N$$

To achieve traceability, our newly proposed signature scheme should not be forged, which was confirmed in our security analysis later in this paper. Furthermore, the incorrect partial signatures should be detected and identified if the signature is suspected forgery.

Theorem 1 If the following congruence relation does not hold, then the false partial signature is detected: $g^{s_i} = (y_{i1})^{\lambda_i \sigma_p} r_i^{HASH} y_{i2}^{\sigma_q} \bmod N$.

Proof This is due to the fact that y_{i1}, y_{i2} is regarded as p_i's public identity. If the participants do not preset bogus secret shadow or tampers with secret shadow, the equation $g^{s_i} = (y_{i1})^{\lambda_i \sigma_p} r_i^{HASH} y_{i2}^{\sigma_q} \bmod N$ must hold because forging s_i equals to solving the difficult discrete logarithm problem.

Group signature generation and verification phase

When all partial signatures from participants in $A=\{p_1, p_1, \ldots, p_l\}$ are valid, the clerk can compute the group signature: $S = \sum_{p_i \in A} s_i \bmod N'$. Thus, $\{m, A, R, S\}$ is the group signature for the message m. Any verifiers can compute:

$$Z = Y^{\sigma_p} \left(\prod_{p_i \in A} y_{i2} \right)^{\sigma_q} \bmod N \tag{11}$$

and then use the group public key $Y = g^{k_1} \bmod N$ to authenticate the validity of $\{m, A, R, S\}$ by checking whether the following equation

$$g^S = ZR^{HASH} \bmod N \tag{12}$$

holds. If so, the group signature $\{m, A, R, S\}$ is valid. The correctness of this equation can be easily seen as follows:

Since $S = \sum_{p_i \in A} s_i \bmod N'$, then

$$S = \sum_{p_i \in A} s_i \bmod p = \sum_{p_i \in A} s_i \bmod q$$

According to Eq.(11), we have

$$S = \sum_{p_i \in A} (s_{p_{i1}} \lambda_i + b_{ip} HASH) \bmod p$$

$$= \sum_{p_i \in A} (s_{p_{i1}} \lambda_i) + \sum_{p_i \in A} (b_{ip} HASH) \bmod p$$

$$= \sum_{p_i \in A} (s_{p_{i1}} \lambda_i) + HASH \sum_{p_i \in A} b_{ip} \bmod p$$

$$= \sum_{p_i \in A} s_{p_{i2}} + HASH \sum_{p_i \in A} b_{iq} \bmod q$$

With the help of σ_p, σ_q, we also have

$$S = \left(\sum_{p_i \in A} (s_{p_{i1}} \lambda_i) + HASH \sum_{p_i \in A} b_{ip} \right) \sigma_p + \left(\sum_{p_i \in A} s_{p_{i2}} + HASH \sum_{p_i \in A} b_{iq} \right) \sigma_q \bmod N'$$

$$= k_1 \sigma_p + HASH \left(\sigma_p \sum_{p_i \in A} b_{ip} + \sigma_q \sum_{p_i \in A} b_{iq} \right) + \sigma_q \sum_{p_i \in A} s_{p_{i2}} \bmod N'$$

Obviously,

$$g^S = \left(g^{k_1 \sigma_p} g^{\sigma_q \sum_{p_i \in A} s_{p_{i2}}} \right) g^{\left(\sigma_p \sum_{p_i \in A} b_{ip} + \sigma_q \sum_{p_i \in A} b_{iq} \right) HASH} \bmod N$$

$$= \left(Y^{\sigma_p} \prod_{p_i \in A} g^{s_{p_{i2}} \sigma_q} \right) g^{\sum_{p_i \in A} (\sigma_p b_{ip} + \sigma_q b_{iq}) HASH} \bmod N$$

$$= \left(Y^{\sigma_p} \prod_{p_i \in A} y_{i2}^{\sigma_q} \right) g^{HASH \sum_{p_i \in A} b_i} \bmod N$$

$$= Z \prod_{p_i \in A} r_i^{HASH} \bmod N = ZR^{HASH} \bmod N$$

The signers are anonymous to the verifier because it is not possible to find out the identities of the

signers in A from the group signature.

SECURITY ANALYSIS

The security of the proposed scheme is based on well-known cryptographic assumptions: the intractability of reversing the one-way hash function (OWHF) and solving the discrete logarithm (DLP). Conspiracy and forgery attacks mentioned by Michels and Horster (1996) as scheme proposed by Desmedt and Frankel (1992b), Li *et al*.(1995), and Harn (1994a) cannot break our scheme.

Theorem 2 The secret is secure, and this new scheme is invulnerable to conspiracy attacks.

Proof Attackers who try to pirate the secret k_1 may include any outside adversaries and inside participants in A.

Attack 1 Some participants in A may cooperate to reveal k_1. Only when all the participants in the authorized subset A cooperate with each other, can they recover k_1 through the equation $k_1=\lambda_1 s_{p_{i1}}+\lambda_2 s_{p_{2i}}+\cdots+\lambda_l s_{p_{li}}$. Any other participants in subset $A'=\{p_1, p_2, \ldots, p_{l'}\}\notin T$ who try to pirate k_1 must resolve $k_1=\boldsymbol{v}_1\cdot\psi(D)$ as follow:

$$\begin{cases} s_{p_{i1}}=\boldsymbol{v}_1\cdot\psi(p_1) \\ s_{p_{2i}}=\boldsymbol{v}_1\cdot\psi(p_2) \\ \cdots \\ s_{p_{l'i}}=\boldsymbol{v}_1\cdot\psi(p_{l'}) \end{cases}, \quad \begin{cases} s_{p_{i2}}=\boldsymbol{v}_2\cdot\psi(p_1) \\ s_{p_{i2}}=\boldsymbol{v}_2\cdot\psi(p_2) \\ \cdots \\ s_{p_{l'i2}}=\boldsymbol{v}_2\cdot\psi(p_{l'}) \end{cases},$$

$$\boldsymbol{v}_2\cdot\psi(D)=(\boldsymbol{v}_1\cdot\psi(D))^2,$$

where $\psi(D)\notin<\psi(p_1), \ldots, \psi(p_{l'})>$. Since $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ is kept secret for them in our scheme, no member in $A'=\{p_1, p_1, \ldots, p_{l'}\}$ will get any useful information about k_1. Similarly, when $A'=\{p_1, p_1, \ldots, p_{l-1}\}\subset A$ is a set of cheaters who do not know k_1, each p_i in A' may show his faulty shadow pair $(s'_{p_{i1}}, s'_{p_{i2}})=(s_{p_{i1}}+\varepsilon_i, s_{p_{i2}}+\delta_i)$, ($i$=1, 2, …, l–1), where $\varepsilon,\delta\in K$, $\varepsilon\neq 0$ if he wishes to resolve k'_1 through the following equations

$$k'_1=\sum_{i=1}^{l}\lambda_i s_{p_{i1}}+\sum_{i=1}^{l-1}\lambda_i\varepsilon_i=k_1+\varepsilon,$$

$$k'_2=\sum_{i=1}^{l}\lambda_i s_{p_{i2}}+\sum_{i=1}^{l-1}\lambda_i\delta_i=k_2+\delta.$$

Evidently, these cheaters cannot be detected only if $k_1^2+\delta=(k_1+\varepsilon)^2$, that is, $\delta=\varepsilon^2+2k_1\varepsilon$. As a result, the probability that cheaters succeed with faulty (ε, δ) is only $1/q^2$.

Attack 2 An outside adversary tries to reveal k_1. He has to resolve k_1 through the public key $Y=g^{k_1} \bmod N$. Obviously, that equals solving DLP.

Theorem 3 Secret keys for each participant are secure.

Proof As we know, in the distribution of secret shadows and verification phase, only each p_i's public keys $y_{i1}=g^{s_{p_{i1}}} \bmod N$ and $y_{i2}=g^{s_{p_{i2}}} \bmod N$ are public. Attackers cannot pirate x_{i1}, x_{i2} through other ways. It implies that revealation of x_{i1}, x_{i2} by a cheater equals solving DLP.

Theorem 4 Forgery attackers will not succeed.

Proof Firstly, we implement two types of signature in two channels (one type in each channel). Malicious users can forge the signature only if the signatures in both p channel and q channel can be forged. Instead of attaching a random number to the secret key held by each member (Li *et al*., 1995), this new scheme can withstand conspiracy attacks. The attack described in (Michels and Horster, 1996) may succeed in forging the p channel signatures. However, the q channel signature can avoid this attack since we apply a hash function to the signed messages m and R. This countermeasure can avoid the attack mentioned by Michels and Horster (1996). In fact, we directly adopt the signature scheme proposed in Michels and Horster (1996)'s scheme (refer to its heuristic countermeasures) as our q channel signature; thus, our scheme can withstand the attack presented by Michels and Horster (1996).

Furthermore, we can check the security of our scheme by resolving the questions given by Li *et al*.(1995). We omit detailed analysis here because it is very similar to the latter. The reader may refer to that solution for more detailed information.

Let us consider the case where two members p_i and p_j conspire with each other to change the group signature $\{m, A, R, S\}$ into $\{m, A', R', S'\}$, where $p_i\in A$, $p_j\notin A$, $S'=S-s_{p_{i2}}\sigma_q+s'_{p_{i2}}\sigma_q$, $R'=R$, $A'=A-p_i+p_j$. In this case, the clerk will reject (A')'s legality without verification of each participant's partial signature. The reason is that $HASH=h(m, R, A)$

includes the information about the authorized set A. For participants, the signed message is $HASH=h(m, R, A)$. On the other hand, for the clerk, he will compute $HASH'=h(m, R', A')$ first and then compute $Z'R'^{HASH'}$, where $Z'=Y^{\sigma_p}\left(\prod_{p_i\in A'} y_{i2}\right)\sigma_q \bmod N$. Since $HASH\neq HASH'$, it is impossible that $g^{S'}=Z'R'^{HASH'}$. Consequently, we can save the cost of partial signature verification.

Table 1 shows comparison of signature scheme in terms of inherent properties. From this table, we know that our scheme does not need to determine signers and signing order in advance, although we should determine the authorized subset A first.

EFFICIENCY ANALYSIS

Data from Table 1 tell us our scheme is similar to that proposed by Li *et al*.(1995) in terms of properties. So in this Section, we will analyze the new proposed scheme's efficiency, and compare it with that proposed by Li *et al.*(1995).

Let T_e, T_m be the time complexity for computing 160 bits of exponentiation and multiplication, respectively. Because all the exponents except S in our scheme never exceed 160 bits and we assume that the prime factor q is also 160 bits in Li *et al*.(1995)'s scheme, we may further compare the performance between these two schemes. Considering the computational cost, we need only $2T_e+tT_m$ and $3T_e+T_m$ to compute the public verification value Z and to verify the signature, where computing g^S consumes $2T_e$. Similarly, in Li *et al*.(1995)'s scheme, we need $t(T_e+T_m)$ and $2(T_e+T_m)$ to compute T and to verify the signature. We optimize in advance the signature generation process (refer to Li *et al*.'s expression of T and Z in our scheme), and omit $(t-3)T_e+T_m$ in terms of computational cost. Considering the storage cost, we need $O(N+p+q)$ to store both public and secret keys. While in Li *et al*.(1995)'s scheme, $O(2p+q)$ is needed. According to its assumption, we need 834 bits to store the keys while scheme in Li *et al*.'s scheme needs 1184 bits. Moreover, we can reduce the storage cost of each member's public key pair (y_{i1}, y_{i2}) using the Chinese Remainder Theorem as follows:

Let $Y_i=g^{s_{p_{i1}}\sigma_p s_{p_{i2}}\sigma_q} \bmod N$, then we have: $\begin{cases} y_{i1}=Y_i^q \bmod N \\ y_{i2}=Y_i^p \bmod N \end{cases}$. Integrating two public keys y_{i1} and y_{i2} into a single public key Y_i reduces the storage cost by half. However, there is a potential drawback in increasing the computational cost. To derive (y_{i1}, y_{i2}) from Y_i, we need some extra computation.

Considering the communication cost, in the group signature generation process, we need $O(n)$ for participants to communicate with the clerk, which is the almost the same as that in scheme proposed by Okamoto (1988), Li *et al*.(1995), Desmedt and Frankel (1992a), while in scheme proposed by Harn and Kiesler (1989), Harn (1994b), we need $O(n^2)$.

Table 2 compares signature scheme in terms of computational complexity.

Obviously, our scheme is more efficient than other similar schemes in terms of verifying the group signature.

CONCLUSION

By implementing the signatures in two channels

Table 1 Properties comparison

	Scheme	Type	Signing order predetermined	Signers determined in advance	Traceability property
Multi-signature	Harn and Kiesler (1989)	S	Yes	Yes	No
	Okamoto (1988)	S	No	No	No
	Harn (1994b)	P	No	Yes	Yes
Threshold multi-signature	Li *et al*.(1995)	P	No	No	Yes
	Desmedt and Frankel (1992a)	P	No	No	No
Vector space secret sharing based multi-signature	Proposed	P	No	No	Yes
Distributed RSA signature for general access structure	Herranz *et al*.(2003)	P	No	No	No

S–Serial digital multi-signature scheme; P–Parallel digital multi-signature scheme

Table 2 Computational complexity comparison

Scheme	Modulo multiplication	Modulo exponentiation	Inverse computation
Li *et al*.(1995)	t+2	t+2	0
Harn (1994a)	t	2t+3	t–1
Desmedt and Frankel (1992a)	t+1	0	0
Herranz *et al*.(2003)	t	t+3	0
Proposed	t+1	5	0

and choosing the system parameters carefully, we built an efficient multi-signature scheme that extended the ordinary threshold signature scheme successfully. In the new scheme, conspiracy and forgery attackers cannot succeed. We also simplified the group signature verification process, but still ensured its anonymity and traceability.

Furthermore, this new scheme achieves good extensibility. When applying vector space secret sharing scheme proposed by Xu *et al.*(2002) into our solution, we can easily construct a three-channel multi-signature, which will strengthen the security more but without loss of its property of anonymity and traceability. Because of space limitation, we will not describe such extended scheme here.

Similarly, we can even extend our scheme into one that is implemented in n channels, if necessary. Analysis of its feasibility, security and efficiency still remains our future work.

References

Brickell, E.F., 1989. Some ideal secret sharing schemes. *Journal of Combin Math and Combin Comput*, **9**:105-113.

Desmedt, Y., Frankel, Y., 1992a. Parallel Reliable Threshold Multi-signature. Technical Report TR-92-04-02, http://citeseer.nj.nec.com/frankel92parallel.html.

Desmedt, Y., Frankel, Y., 1992b. Shared Generation of Authenticators and Signatures. Advances in Cryptology-Crypto'91. Springer, Berlin, p.457-469.

Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T., 1996. Robust Threshold DSS Signature. Advances in Cryptology-Eurocrypto'96. Springer, Berlin, p.354-371.

Harn, L., 1994a. Group-oriented (*t*,*n*) threshold digital signature scheme and multisignature. *IEEE Proc Computers and Digital Tech*, **141**(5):307-313.

Harn, L., 1994b. New digital signature scheme based on discrete logarithm. *Electron Lett*, **26**(5):296-298.

Harn, L., Kiesler, T., 1989. New scheme for digital multisignature. *Electron Lett*, **25**(15):1002-1003.

Herranz, C., Padró, C., Sáez, G., 2003. Distributed RSA Signature Schemes for General Access Structures. Information Security Conference (ISC'03). LNCS.2851, Bristol, United Kingdom, p.123-137.

Li, C., Hwang, T., Lee, N., 1994. Remark on the Threshold RSA Signature Scheme. Advances in Cryptology-Crypto'93, Lecture Notes in Computer Science, p.773.

Li, C., Hwang, T., Lee, N., 1995. Threshold-multisignature Schemes Where Suspected Forgery Implies Traceability of Adversarial Shareholders. Advances in Cryptology-Eurocrypt'94. Springer, Berlin, p.194-204.

Michels, M., Horster, P., 1996. On the risk of disruption in several multiparty signature schemes. *Proc of the International Conference on the Theory and Applications of Cryptology and Information Security*, **3**(7):334-345.

Okamoto, T., 1988. A digital multisignature scheme using bijective public key cryptosystems. *ACM Trans Comput Syst*, **6**(8):432-441.

Padró, C., Sáez, G., 1999. Detection of cheaters in vector space secret sharing schemes. *Designs, Codes and Cryptoraphy*, **16**(1):75-85.

Safavi, N.R., Wang, H., Lam, K.Y., 1999. A New Approach to Bobust Threshold RSA Signature Schemes. Information Security and Cryptology-ICISC'99. Springer, Korea, p.184-196.

Stinson, D.R., 1995. Cryptography: Theory and Practice. CRC Press, Florida, p.343-350.

Tompa, M., Woll, H., 1988. How to share a secret with cheaters. *Journal of Cryptology*, **1**(2):133-138.

Ventzislav, N., Svetla, N., Bart, P., Joos, V., 2001. Applying General Access Structure to Proactive Secret Sharing schemes. http://www.esat.kuleuven.ac.be/~snikova/svbj_benelux02.pdf.

Xu, C.X., Chen, K., Xiao, G.Z., 2002. A secure vector space secret sharing scheme. *ACTA ELECTRONICA SINICA*, **30**(5):715-718.