Consideration for multi-threshold multi-secret sharing schemes

Atsushi Waseda
National Institute of Information and
Communications Technology
4-2-1, Nukui-Kitamachi, Koganei, Tokyo,
184-8795, Japan

Masakazu Soshi
Hiroshima City University
3-4-1, Ozuka-Higashi, Asa-Minami-Ku, Hiroshima,
731-3194, Japan

***Abstract*—In this paper, we propose the new (t_i, n) threshold multi secret sharing scheme. In our scheme, each user keeps only one share and the secret vectors $K_i = \{k_{i,1}, \ldots, k_{i,m_i}\}$ are shared according to independent (t_i, n) threshold access structures ($i = 1, \ldots, h$). Here note that a (t_i, n) threshold multi-secret sharing scheme has been proposed by Shi et al. [1]. Unfortunately, however, there is a serious attack on Shi's scheme that can reconstruct all elements of K_i with only t_1 shares. In this paper, we shall give the solution to this problem by using one-way functions. Furthermore, Shi's scheme has a drawback such that the dimension of the secret vector K_i cannot exceed t_i. On the other hand, our scheme has no such a restriction. Finally, we demonstrate that our scheme is more efficient than Shi's scheme by showing that our scheme is more efficient than the three naive improvements on the protocol of Shi et al.**

I. Introduction

Secret sharing scheme (SSS) is a method to share secret information among a set of participants, each of which is given a share of the secret by a dealer. In 1979, Shamir [2] and Blakley [3] first proposed (t, n) threshold SSS, independently. In a (t, n) threshold scheme, at least (or any) t of the n shares can reconstruct the secret, while any set of less than t shares can give no information about it at all. So far many SSSs including verifiable SSSs (VSSSs) [4], [5], multi-secret sharing schemes (MSSSs) [6], [7] and quantum SSSs (QSSSs) [8], [9] have been proposed. VSSS is a secret sharing scheme which is able to verify that every share is correctly constructed by the dealer (or Trusted Third Party (TTP)). QSSS is implemented by using quantum mechanics for secret sharing. In MSSS, there are multiple secrets to be shared during one secret sharing process.

He and Dawson proposed a multi-stage secret sharing scheme which is a sort of MSSS [10]. In this scheme, many secrets are shared but only one share is kept by each user. Its reconstruction rule is the same as (t, n) threshold scheme. However, in the scheme many secrets must be reconstructed stage-by-stage in a predetermined order by the dealer. When all the secrets have been reconstructed, the dealer can use the public shift technique so as not to redistribute new shares to each user. The number of public values of this scheme is $m \cdot n$, where m is the number of secrets and n is the number of users. In 1995, Harn improved the multi-stage secret sharing scheme proposed by He and Dawson by reducing the number of public values to $m \cdot (n - t)$ [11]. In 2000, Chien et al. proposed a new multi-secret sharing scheme based on systematic block codes [12]. In their scheme each user keeps one share and all the secrets can be reconstructed according to (t, n) threshold scheme at the same time. The number of public values of this scheme is $m + n - t + 1$. In 2008, Shi et al. proposed (t_i, n) threshold multi-secret sharing schemes ($i = 1, \ldots, h$, $t_1 < t_2 < \cdots < t_h$) [1]. In this scheme, each secret vector K_i is shared according to the independent (t_i, n) threshold access structure ($i = 1, \ldots, h$). The number of each user's shares is one. Moreover the number of public values is $n \cdot t_h$. Note that any kind of unconditionally secure multi-stage secret sharing is impossible due to the information theoretic lower bound given in [12].

In this paper, we propose the new (t_i, n) threshold multi-secret sharing scheme. In Shi's scheme, unfortunately, there is a serious attack that can reconstruct all elements of K_i with only t_1 shares. Our scheme gives the solution to this problem by using one-way functions. Moreover, Shi's scheme has a severe limitation such that the dimension of the secret vector K_i cannot exceed t_i. Our scheme is able to free up this restriction and thus can distribute secret vectors K_i of arbitrary dimensions m_i ($i = 1, \ldots, h$). Furthermore, in our scheme, each user keeps only one share and K_i are shared according to independent (t_i, n) threshold access structures ($i = 1, \ldots, h$). The number of public values of our protocol is

$$n \cdot t_h + m + 1 \tag{1}$$

with $m = \sum_i m_i$, which is superior to naive improvements of the scheme proposed by Shi et al.

This paper is organized as follows. In section 2, we introduce the (t_i, n) threshold multi-secret sharing protocol proposed by Shi et al. and the problem. In section 3, we propose the scheme to overcome the problem. In section 4, we examine the security of our proposed scheme and compare with simple improvements of Shi's protocols. Finally in section 5 we conclude this paper.

II. Previous work

In this section, we introduce a multi-secret sharing scheme proposed by Shi et al. [1]. Let $K_1, \ldots, K_h$ denote h secret vectors on $\mathbb{Z}_q$ (q is a large prime number) and be shared among n participants such that each K_i will be reconstructed according to independent (t_i, n) threshold access structure. Suppose $t_1 < t_2 < \cdots < t_h$. Furthermore, let K_i be $(k_{i,1}, \ldots, k_{i,t_i})^\top$, where $\top$ means the transpose operator. Thus K_i consists of t_i secrets ($i = 1, \ldots, h$). We assume that there exists a secret channel between the dealer and each participant, and the dealer creates a public bulletin board. Now this protocol has two phases: distribution phase and reconstruction phase.

Distribution phase

1. Randomly choose $n \times t_1$ matrix M_1 on $\mathbb{Z}_q$, such that the rank of any $t_1 \times t_1$ sub-matrix of matrix M_1 is t_1, that is, all $t_1 \times t_1$ sub-matrices of M_1 are invertible.
2. Compute the share vector $(s_1, \ldots, s_n)^\top$ as follows:

$$M_1 K_1 = \begin{pmatrix} m_{1,1} & \cdots & m_{1,t_1} \\ \vdots & \ddots & \vdots \\ m_{n,1} & \cdots & m_{n,t_1} \end{pmatrix} \begin{pmatrix} k_{1,1} \\ \vdots \\ k_{1,t_1} \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}. \quad (2)$$

3. For $i = 2$ to h do
Generate $n \times t_i$ matrix M_i

$$M_i = \begin{pmatrix} & m_{1,(t_{i-1}+1)} & \cdots & m_{1,t_i} \\ M_{i-1} & \vdots & \ddots & \vdots \\ & m_{n,(t_{i-1}+1)} & \cdots & m_{n,t_i} \end{pmatrix}, \quad (3)$$

where $m_{j,k} \in \mathbb{Z}_q$, such that the rank of any $t_i \times t_i$ sub-matrix of matrix M_i is t_i, and M_i satisfies the following equation:

$$\begin{aligned} \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \\ &= M_i K_i \\ &= \begin{pmatrix} & m_{1,(t_{i-1}+1)} & \cdots & m_{1,t_i} \\ M_{i-1} & \vdots & \ddots & \vdots \\ & m_{n,(t_{i-1}+1)} & \cdots & m_{n,t_i} \end{pmatrix} \begin{pmatrix} k_{i,1} \\ \vdots \\ k_{i,t_i} \end{pmatrix}. \end{aligned}$$

4. Distribute s_i to every user P_i as her share over the secret channel ($i = 1, \ldots, n$) and put M_h on the public bulletin board.

Reconstruction phase

When t_i or more shares $S_i = \{s_{i_1}, s_{i_2}, \ldots, s_{i_{t_i}}\}$ are collected, we are able to compute inverse matrix $(M_i')^{-1}$ of $t_i \times t_i$ sub-matrix M_i' of matrix M_h and recover K_i as follows:

$$(M_i')^{-1} S_i = (M_i')^{-1} M_i' K_i = K_i. \quad (4)$$

Problem

The serious attack exists in this protocol. When the attacker has $s_1, \ldots, s_{t_1}$, the attacker tries to obtain all the secrets. The attacker obtains the secret $k_{1,1}, \ldots, k_{1,t_1}$ by the reconstruction phase in case of threshold t_1. Then, the attacker is able to calculate the share $s_{t_1+1}, \ldots, s_n$ since M_1 is public. Therefore, the attacker obtains the secret K_i by running the reconstruction phase of threshold t_i.

As the second problem, the dimension of the secret vector K_i is fixed to t_i ($i = 1, \ldots, h$). Moreover, this protocol cannot distribute two or more secret vectors of the same threshold. Thus a secret vector of an arbitrary dimension cannot be distributed. Therefore we shall improve this protocol so that the dealer can distribute secret vectors of arbitrary dimensions.

Naive improvements

Here in order to consider whether or not it is easy to solve the second problem, we discuss three naive improvements on the protocol of Shi et al. Let the length of the secret vector K_i denote m_i ($i = 1, \ldots, h$).

1) Repeat the protocol
Let $A = \max_i\{\lceil m_i/t_i \rceil\}$. A secret vector K_i is divided into $K_{i,1} = (k_{i,1}, \ldots, k_{i,t_i})^\top$, $K_{i,2} = (k_{i,t_i+1}, \ldots, k_{i,2t_i})^\top$, $\cdots$, and $K_{i,A} = (k_{i,(A-1)t_i+1}, \ldots, k_{i,At_i})^\top$. Then the protocol of Shi et al. is repeated A times. We are able to repeat the protocol using the same shares. Therefore, the number of shares which are held by each user is one, although, the number of public values becomes $A \cdot n \cdot t_h$. It is likely that the number is prohibitive.
2) Concatenate the secrets
We can generate new secret vectors:

$$K_i' = (k_{i,1} || \ldots || k_{i,A}, k_{i,A+1} || \ldots || k_{i,2A}, \ldots)^\top \quad (5)$$

where operator $||$ is the concatenation and $A = \max_i\{\lceil m_i/t_i \rceil\}$ ($i = 1, \ldots, h$). The new secret vectors K_i' are shared according to the Shi's protocol. Hence the numbers of secret and public values are the same as Shi's protocol, however, these parameter sizes are A times greater than the original.
3) Enlarge M_h
Let $B = \max_i\{(m_i - t_i)\}$. This improvement is enhancement to $(n+B) \times (t_h + B)$ matrix M_h^e from $n \times t_i$ matrix M_h. The distribution phase is as follows:
$0'$. Randomly choose $(n+B) \times B$ matrix M_0^e on $\mathbb{Z}_q$.
$1'$. Generate $(n+B) \times (t_1 + B)$ matrix M_1^e:

$$M_1^e = \begin{pmatrix} & m_{1,1+B} & \cdots & m_{1,t_1+B} \\ M_0^e & \vdots & \ddots & \vdots \\ & m_{n+B,1+B} & \cdots & m_{n+B,t_1+B} \end{pmatrix}, \quad (6)$$

where $m_{j,k} \in \mathbb{Z}_q$, such that the rank of any $(t_1 + B) \times (t_1 + B)$ sub-matrix of matrix M_1 is $t_1 + B$.
$2'$. Randomly choose $B - (m_1 - t_1)$ vector $K_1' = (k_{1,m_1+1}, \ldots, k_{1,t_1+B})^\top$. Compute the share vector $(s_1, \ldots, s_n)^\top$ and public vector $(s_{n+1}, \ldots, s_{n+B})^\top$

as follows:

$$\begin{aligned} & M_1^e(K_1^\top||(K_1')^\top)^\top \\ &= \begin{pmatrix} & m_{1,1+B} & \cdots & m_{1,t_1+B} \\ M_0^e & \vdots & \ddots & \vdots \\ & m_{n+B,1+B} & \cdots & m_{n+B,t_1+B} \end{pmatrix} \begin{pmatrix} k_{1,1} \\ \vdots \\ k_{1,m_1} \\ k_{1,m_1+1} \\ \vdots \\ k_{1,t_1+B} \end{pmatrix} \\ &= \begin{pmatrix} s_1 \\ \vdots \\ s_n \\ s_{n+1} \\ \vdots \\ s_{n+B} \end{pmatrix}. \end{aligned}$$

$3'$. For $i = 2$ to h do

Randomly choose $B - (m_i - t_i)$ vector $K_i' = (k_{i,m_i+1}, \ldots, k_{i,t_i+B})^\top$ and generate $(n+B) \times (t_i + B)$ matrix M_i^e

$$M_i^e = \begin{pmatrix} & m_{1,(t_{i-1}+1)} & \cdots & m_{1,t_i} \\ M_{i-1}^e & \vdots & \ddots & \vdots \\ & m_{n,(t_{i-1}+1)} & \cdots & m_{n,t_i} \end{pmatrix}, \tag{7}$$

where $m_{j,k} \in \mathbb{Z}_q$, such that the rank of any $(t_i + B) \times (t_i + B)$ sub-matrix of matrix M_i^e is $t_i + B$, and M_i satisfies the following equation:

$$\begin{aligned} & \begin{pmatrix} s_1 \\ \vdots \\ s_n \\ s_{n+1} \\ \vdots \\ s_{n+B} \end{pmatrix} \\ &= M_i^e(K_i^\top||(K_i')^\top)^\top \\ &= \begin{pmatrix} & m_{1,(t_{i-1}+1+B)} & \cdots & m_{1,t_i+B} \\ M_{i-1}^e & \vdots & \ddots & \vdots \\ & m_{n+B,(t_{i-1}+1+B)} & \cdots & m_{n+B,t_i+B} \end{pmatrix} \\ & \cdot \begin{pmatrix} k_{i,1} \\ \vdots \\ k_{i,m_i} \\ k_{i,m_i+1} \\ \vdots \\ k_{i,t_i+B} \end{pmatrix}. \end{aligned}$$

$4'$. Distribute s_i to every user P_i as her share over the secret channel ($i = 1, \ldots, n$) and put M_h^e and $(s_{n+1}, \ldots, s_{n+B})^\top$ on the public bulletin board.

In the reconstruction phase, if $S_i = \{s_{i_1}, s_{i_2}, \ldots, s_{i_{t_i}}\}$ are collected, then we have $s_{i_1}, s_{i_2}, \ldots, s_{i_{t_i}}, s_{n+1}, \ldots, s_{n+B}$ and can compute inverse matrix $((M_i^e)')^{-1}$ of $(t_i + B) \times (t_i + B)$ sub-matrix $(M_i^e)'$ of matrix M_h^e and can recover K_i. Therefore, although the number of share which are held by each user remains one, the number of public values is $(n + B) \cdot (t_h + B) + B$. Again the cost of this case could be too expensive.

Now it should be clear that the three naive schemes cannot solve the problem given before and that it is challenging to give the solution.

III. Our scheme

In this section, we propose a new (t_i, n) threshold secret sharing scheme. Let $K_i = \{k_{i,1}, \ldots, k_{i,m_i}\}$ $(i = 1, \ldots, h)$ be h secret vectors on $\mathbb{Z}_q$ (q is a large prime number). Furthermore, let us suppose that K_i's are shared among n participants such that each K_i will be reconstructed according to independent (t_i, n) threshold access structure $(i = 1, \ldots, h)$. In particular, the dimension of the secret vector K_i is given by m_i which is independent of t_i $(i = 1, \ldots, h)$. Suppose $t_1 < t_2 < \cdots < t_h$. We also assume that there is a secret channel between the dealer and each participant, and the dealer creates a public bulletin board.

Now our protocol consists of two phases: distribution phase and reconstruction phase.

Distribution phase

1. Generate shares $s_1, \ldots, s_n$.

2. Randomly choose a one-way function f_1 and a vector $R_1 = (r_{1,1}, r_{1,2}, \ldots, r_{1,t_1})^\top$. Randomly choose $n \times t_1$ matrix M_1 on $\mathbb{Z}_q$, such that M_1 satisfies the following relationship:

$$M_1 R_1 = \begin{pmatrix} m_{1,1} & \cdots & m_{1,t_1} \\ \vdots & \ddots & \vdots \\ m_{n,1} & \cdots & m_{n,t_1} \end{pmatrix} \begin{pmatrix} r_{1,1} \\ r_{1,2} \\ \vdots \\ r_{1,t_1} \end{pmatrix} = \begin{pmatrix} f_1(s_1) \\ \vdots \\ f_1(s_n) \end{pmatrix}, \tag{8}$$

and the rank of any $t_1 \times t_1$ sub-matrix of matrix M_1 is t_1, that is, all $t_1 \times t_1$ sub-matrices of M_1 are invertible.

3. For $i = 2$ to h do

Generate a one-way function f_i, a random vector $R_i = (r_{i,1}, r_{i,2}, \ldots, r_{i,t_i})^\top$ and $n \times t_i$ matrix M_i:

$$M_i = \begin{pmatrix} & m_{1,(t_{i-1}+1)} & \cdots & m_{1,t_i} \\ M_{i-1} & \vdots & \ddots & \vdots \\ & m_{n,(t_{i-1}+1)} & \cdots & m_{n,t_i} \end{pmatrix}, \tag{9}$$

where $m_{j,k} \in \mathbb{Z}_q$, such that the rank of any $t_i \times t_i$ sub-matrix of matrix M_i is t_i, and M_i satisfies the following relationship:

$$\begin{aligned} & \begin{pmatrix} f_i(s_1) \\ \vdots \\ f_i(s_n) \end{pmatrix} \\ &= M_i R_i \\ &= \begin{pmatrix} & m_{1,(t_{i-1}+1)} & \cdots & m_{1,t_i} \\ M_{i-1} & \vdots & \ddots & \vdots \\ & m_{n,(t_{i-1}+1)} & \cdots & m_{n,t_i} \end{pmatrix} \begin{pmatrix} r_{i,1} \\ r_{i,2} \\ \vdots \\ r_{i,t_i} \end{pmatrix}. \end{aligned}$$

4. Compute $C = \{c_{1,1}, \ldots, c_{1,m_{t_1}}, c_{2,1}, \ldots, c_{h,m_h}\}$

$$\begin{aligned}
&c_{1,1} \\
&\quad = \sum_{i=1}^{m_1} k_{1,i} g^{0(i-1)} + \sum_{i=1}^{t_1} r_{1,i} g^{0(m_1-1+i)}, \\
&\quad \vdots \\
&c_{1,m_1} \\
&\quad = \sum_{i=1}^{m_1} k_{1,i} g^{(m_1-1)(i-1)} + \sum_{i=1}^{t_1} r_{1,i} g^{(m_1-1)(m_{1-1+i})}, \\
&c_{2,1} \\
&\quad = \sum_{i=1}^{m_2} k_{2,i} g^{m_1(i-1)} + \sum_{i=1}^{t_2} r_{2,i} g^{m_1(m_2-1+i)}, \\
&\quad \vdots \\
&c_{2,m_2} \\
&\quad = \sum_{i=1}^{m_2} k_{2,i} g^{(m_1+m_2-1)(i-1)} \\
&\qquad + \sum_{i=1}^{t_2} r_{2,i} g^{(m_1+m_2-1)(m_2-1+i)}, \\
&\quad \vdots \\
&c_{j,l} \\
&\quad = \sum_{i=1}^{m_j} k_{j,i} g^{(\sum_{p=1}^{j-1} m_p+l-1)(i-1)} \\
&\qquad + \sum_{i=1}^{t_j} r_{j,i} g^{(\sum_{p=1}^{j-1} m_p+l-1)(m_j-1+i)}, \\
&\quad \vdots \\
&c_{h,m_h} \\
&\quad = \sum_{i=1}^{m_h} k_{h,i} g^{(m-1)(i-1)} + \sum_{i=1}^{t_h} r_{h,i} g^{(m-1)(m_h-1+i)},
\end{aligned}$$

with g being a primitive element in $\mathbb{Z}_q$ and $m = \sum_i m_i$.
5. Distribute s_i to each participant P_i as her share over the secret channel and put M_h, $c_{j,l}$, f_j and g on the public bulletin board.

Reconstruction phase

When t_i or more shares $S_i = \{s_{i_1}, s_{i_2}, \ldots, s_{i_{t_i}}\}$ are collected, we are able to compute inverse matrix $(M_i')^{-1}$ of $t_i \times t_i$ sub-matrix M_i' of matrix M_h and recover $r_{i,1}, \ldots, r_{i,t_1}$. Then, $c_{i,1}, \ldots, c_{i,m_i}$ have m_i unknown symbols. So, the secrets $k_{i,1}, \ldots, k_{i,t_i}$ are reconstructed by solving $c_{i,1}, \ldots, c_{i,m_i}$.

IV. Security analysis and comparison

In this section, we examine the security of our scheme and then compare the features of different schemes.

Reconstruction of the secret K_i using t_i shares

When $S_i = \{f_i(s_{i_1}), f_i(s_{i_2}), \ldots, f_i(s_{i_{t_i}})\}$ are collected, we are able to compute inverse matrix $(M_i')^{-1}$ of $t_i \times t_i$ sub-matrix M_i' of matrix M_h and recover $R_i = r_{i,1}, \ldots, r_{i,t_i}$ as follows:

$$(M_i')^{-1} S_i = (M_i')^{-1} M_i' R_i = R_i. \tag{10}$$

In this case the participants can determine the values of the secrets uniquely since the number of the missing symbols is equal to the number of equations $c_{i,1}, \ldots, c_{i,m_i}$.

Security of shares

If there are $P_1, \ldots, P_{t_i-1}$ trying to obtain share of P_{t_i}, they cannot uniquely determine the values of s_{t_i} since the number of unknown symbols $f_i(s_{t_i}), R_i$ is larger than linear equation of sub-matrix M_i' of matrix M_i corresponding to their shares. In another attack, the attackers obtain R_{i-1} by reconstruction step of the secret corresponding to threshold t_{i-1}, and $f_{i-1}(s_{t_i})$ by calculating $M_{i-1}R_{i-1}$. However, since f_{i-1} is one-way function, the attackers cannot obtain the share s_{t_i}.

Security of secrets

Given public values $c_{i,1}, \ldots, c_{i,m_i}$ for reconstructing K_i, an adversary has no way to derive the secrets since the number of unknown symbols $k_{i,1}, \ldots, k_{i,m_i}, r_{i,1}, \ldots, r_{i,t_i}$ is larger than the number of linear equations in $c_{i,1}, \ldots, c_{i,m_i}$. If there are t ($< t_i$) members trying to solve the equation of $c_{i,1}, \ldots, c_{i,m_i}$, they cannot uniquely determine the values of $r_{i,1}, \ldots, r_{i,t_i}$ since the number of missing symbols is larger than linear equation of sub-matrix M_i' of matrix M_h corresponding to their shares. Thus they are not able to determine the secret values uniquely.

Our scheme, therefore, enforces the (t_i, n) secret sharing rule.

Comparison with naive improvements

With respect to the size of public values, we compare our scheme with the naive improvement schemes of [1], which are given in section II. Let $A = \max_i\{\lceil m_i/t_i \rceil\}$, $B = \max_i\{(m_i - t_i)\}$ and $m = \sum_i m_i$. The number of public values in our scheme is $n \cdot t_h + m + 1$. Since each parameter is $\log q$ bits, the size of the public values in our scheme is $(n \cdot t_h + m + 1) \log q$ bits. Note that f_i is also public in our protocol. However these must be applied also to naive improvements in order to secure against the attack. Therefore, f_i is omitted in the following comparison. In the naive scheme 1) in section II, since the number of the public values is $A \cdot n \cdot t_h$ and the size of each parameter is $\log q$ bits, the size of the public values is $(A \cdot n \cdot t_h) \log q$ bits in total. In the second naive scheme 2), the number of public values is $n \cdot t_h$. However, each parameter is $A \log q$ bit long. Then, the size of the public values is also $A(n \cdot t_h) \log q$ bits. The public value size of our scheme is smaller than those of the above naive cases, if

$$n \geq \frac{m+1}{t_h(A-1)}. \tag{11}$$

Protocol	multi threshold scheme	dimension of K_i	size of public values
Ours	Yes	arbitrary	$(n \cdot t_h + m + 1) \log q$
Shi et al.[1]	Yes	$\leq t_i$	n/a
naive 1 and 2	Yes	arbitrary	$(A \cdot n \cdot t_h) \log q$
naive 3	Yes	arbitrary	$((n + B) \cdot (t_h + B) + B) \log q$
He et al.[10]	No	-	-
Harn[11]	No	-	-
Chien et al.[12]	No	-	-

TABLE I
COMPARISON WITH PREVIOUS WORKS: $A = \max_i\{\lceil m_i/t_i \rceil\}$, $B = \max_i\{(m_i - t_i)\}$ AND $m = \sum_i m_i$.

In the naive scheme 3), since the number of public values is $(n+B)\cdot(t_h+B)+B$ and the size of each parameter is $\log q$ bits, the size of the public values is $((n+B)\cdot(t_h+B)+B)\log q$ bits. The public value size of our scheme is smaller than this case, if

$$n \geq \frac{m+1}{B} - (t_h + B + 1). \qquad (12)$$

Therefore, our protocol is more efficient than the naive improvements of Shi's protocol in many cases. For example, if $t_1 = 2, t_{i+1} = t_i + 1 (i = 1, \ldots, h-2), t_h = n, m_i = n (i = 1, \ldots, n-1)$, for arbitrary n the public value size of our scheme is smaller than the three naive improvements above. Furthermore, our protocol has the advantage to be able to share the secrets of many different threshold values in one sharing process. The schemes proposed by He et al., Harn and Chien et al. do not have such a feature.

We summarize comparison of our scheme with previous works in Table 1. Note that in Table 1 it is difficult to compute the size of public values in Shi's scheme because the scheme is not a multi-threshold protocol with secret vectors of arbitrary dimensions as ours.

V. Conclusion

In this paper, we have proposed the new (t_i, n) threshold multi secret sharing scheme. A (t_i, n) threshold multi-secret sharing scheme has been proposed by Shi et al. In Shi's scheme, unfortunately, there is a serious attack that can reconstruct all elements of K_i with only t_1 shares. Our scheme gives the solution to this problem by using one-way functions. Moreover, Shi's scheme has a severe limitation such that the dimension of the secret vector K_i cannot exceed t_i. Our scheme is able to free up this restriction and thus can distribute secret vectors K_i of arbitrary dimensions m_i $(i = 1, \ldots, h)$. Furthermore, our scheme is more efficient than the three naive improvements on the protocol proposed by Shi et al. in general.

References

[1] R. Shi, L. Huang, Y. Luo, and Z. Hong, "A threshold multi-secret sharing scheme," in *IEEE International Conference on Networking, Sensing and Control, ICNSC*, 2008, pp. 1705–1707.

[2] A. Shamir, "How to share a secret," in *Comm. ACM 22*, 1979, p. 612.

[3] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS 1979 National Computer Conference*. AFIPS, 1979, pp. 313–317.

[4] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *FOCS*, 1987, pp. 427–437.

[5] A. Patra, A. Choudhary, T. Rabin, and C. Rangan, "The round complexity of verifiable secret sharing revisited," in *Advances in Cryptology - CRYPTO 2009*, ser. Lecture Notes in Computer Science, S. Halevi, Ed. Springer Berlin / Heidelberg, 2009, vol. 5677, pp. 487–504.

[6] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe, "Multisecret threshold schemes," in *CRYPTO '93*, 1993, pp. 126–135.

[7] C. Blundo, A. D. Santis, G. D. Crescenzo, A. G. Gaggia, and U. Vaccaro, "Multi-secret sharing schemes," in *Advances in Cryptology – CRYPTO '94*, 1994, pp. 150–163.

[8] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, no. 3, pp. 1829–1834, March 1999.

[9] F.-L. Yan, T. Gao, and Y.-C. Li, "Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations," *Chinese Phys. Lett*, vol. 25, pp. 1187–1190, 2008.

[10] J. He and E. Dawson, "Multistage secret sharing based on one-way function," *Electronics Letters*, vol. 30, no. 19, pp. 1591–1592, 1994.

[11] L. Harn, "Comment: Multistage secret sharing based on one-way function," *Electronics Letters*, vol. 31, no. 4, p. 262, 1995.

[12] H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, "A practical (t,n) multi-secret sharing scheme," *IEICE Transactions on Fundamentals*, vol. E83-A, no. 12, pp. 2762–2765, 2000.