A (k,t,n) verifiable multi-secret sharing scheme based on adversary structure

Jing Li, Licheng Wang, Jianhua Yan, Xinxin Niu, Yixian Yang
Information Security Center,
State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications,
Beijing, 100876 P.R. China
[e-mail: wanglc2012@126.com]
*Corresponding author: Licheng Wang

Received March 9, 2014; revised September 10, 2014; revised October 13, 2014; accepted October 23, 2014; published December 31, 2014

Abstract

A (n,t,n) secret sharing scheme is to share a secret among n group members, where each member also plays a role of a dealer,and any t shares can be used to recover the secret. In this paper, we propose a strong (k,t,n) verifiable multi-secret sharing scheme, where any k out of n participants operate as dealers. The scheme realizes both threshold structure and adversary structure simultaneously, and removes a trusted third party. The secret reconstruction phase is performed using an additive homomorphism for decreasing the storage cost. Meanwhile, the scheme achieves the pre-verification property in the sense that any participant doesn't need to reveal any information about real master shares in the verification phase. We compare our proposal with the previous (n,t,n) secret sharing schemes from the perspectives of what kinds of access structures they achieve, what kinds of functionalities they support and whether heavy storage cost for secret share is required. Then it shows that our scheme takes the following advantages: (a) realizing the adversary structure, (b) allowing any k out of n participants to operate as dealers, (c) small sized secret share. Moreover, our proposed scheme is a favorable candidate to be used in many applications, such as secure multi-party computation and privacy preserving data mining, etc.

Keywords: (k,t,n) secret sharing, adversary structure, pre-verification property, homomorphism

This work was supported by the National Natural Science Foundation of China (NSFC) (Nos. 61103198, 61121061,61370194), and the NSFC A3 Foresight Program (No. 61161140320).

http://dx.doi.org/10.3837/tiis.2014.12.018

1. Introduction

A secret sharing scheme (SSS) is to share a secret among a group of participants.In such a scheme, any qualified subset of participants, pooling together their shares, can recover the secret; whereas any unqualified subset could not obtain any information about it. Secret sharing schemes [8,12,19-20] have been widely used in practical applications, such as image preserving, implicit data security and e-voting, etc. Secret sharing schemes first introduced by Shamir [24] and Blakley [4] in 1979 were based on Lagrange polynomial interpolation and projective geometry theory, respectively. In threshold schemes, the shared secret can be reconstructed by any t or more than t participants, but any set having less than t participants cannot recover it.

During the past three decades, many threshold SSSs for a variety of features have been presented. In 1999, Lin et. al [16] designed a verifiable threshold multi-secret sharing scheme, based on the intractability of the factorization and the discrete logarithm module a large composite problems. The scheme provides efficient solutions against cheating by the dealer or any participant. In 2000, a multi-secret scheme [5] based on the systematic block codes was proposed. After that, a new multi-secret sharing scheme [27] based on Shamir's secret sharing was constructed in 2004. Compared with the scheme reported in [5], the new proposal in [27] has fewer public parameters and small storage. In 2008, a dynamic threshold multi-secret sharing scheme was given [25], where many secrets are shared in such a way that all secrets can be reconstructed independently without refreshing the shares. Before 2009, while keeping a view on rounds in a SSS, the best known unconditionally secure protocol needs three rounds in sharing phase. Later, Patra et al. [21], by introducing the definition of verification secret sharing with only negligible probability of error, designed a novel protocol that takes only two rounds in sharing phase and two rounds in reconstruction phase. Subsequently, a verification secret sharing scheme [1] within a total of three rounds (only two rounds in sharing and one round in reconstruction) was constructed. In 2014, the first multilevel threshold secret sharing based on Chinese Remainder Theorem was proposed in [10], where each participant keepsonly one private share and the scheme is unconditionally secure. In such a scheme, shareholders are classified into different security subsets. The threshold value of a higher-level subset is smaller than the threshold value of a lower-level subset. However, the aforementioned threshold SSSs need a trusted third party for acting as a dealer.

In 1990, Ingemarsson and Simmons [13] introduced an idea for removing a trusted third party (TTP) in secret sharing, and then presented a simple protocol, where n participants generate shares of the scheme. Subsequently, Pedersen (1991) proposed the first (t,n) threshold secret sharing scheme [22] based on Shamir's SSS. In Pedersen's SSS, each participant also plays a role as a dealer for distributing secret shares to others without the assistance of TTPs. Meanwhile, each one randomly chooses an element, called sub-secret, and then distributes it using Shamir's share generation algorithm to generate the sub-shares for other participants. By the property of additive homomorphism [2] of the reconstruction algorithm, each participant is able to combine all of his sub-shares into a single share, called master secret, which can be recovered with the knowledge of any t or more than t master shares using Lagrange polynomial interpolation. After that, some cryptosystem protocols [15,26] without trusted third parties were proposed. For example, the scheme reported in [26] is a threshold undeniable signature scheme without TTPs. The scheme in [15] shares a quantum secret without TTPs.

In 2010, Harn and Lin [11] presented a strong (n,t,n) verifiable secret sharing scheme (VSSS). Such type of schemes are called (n,t,n) SSS since the first parameter n refers to the number of dealers, the second parameter t refers to the threshold, and the third parameter n refers to the number of participants. Meanwhile, a new concept of strong t-consistency of shares has been introduced by Harn and Lin [11]. In the proposed scheme, it can be verified that all the qualified subsets can recover the same secret. After that, to decrease the number of verification polynomials for improving the efficiency of the scheme, Liu (2012) designed an efficient (n,t,n) VSSS [17], in which participants generate only one verification polynomial for testing the strong t-consistency of shares. Then, Liu's VSSS achieves multi-secret sharing.

In terms of access structures [3,9,14], it can be seen that the access structure of (t,n) threshold SSSs is a special case of general access structures. In 2009, Qin [23] presented a secret sharing scheme that can achieve both the threshold and the adversary structure. However, each participant needs to keep a share of relatively big size $m|S|$, where m is the number of adversary sets and $|S|$ is the size of the shared secret. In order to improve the efficiency, Zhao [28] proposed a new scheme with a share of size $\frac{|S|+|a|}{t}+\frac{(|S|+|a|)(m-1)}{t^2}$, where $|a|$ is the size of populated data. In such schemes [23,28], t or more than t participants are able to recover the shared secret in general, meanwhile some subsets of parties that each containing at least t participants cannot reconstruct the shared secret. Thus, the scheme can efficiently restrict the powers of participants. Finally, inspiring from the ideas proposed in [17, 28], our motivation is to design an improved SSS that can support adversary structure and remove the involvement of trusted third parties simultaneously.

Contributions. This paper presents a strong (k,t,n) verifiable multi-secret sharing scheme that removes a mutually trusted third party. Here, the first parameter k refers to the number of dealers, the second parameter t refers to the threshold value, and the third parameter n refers to the number of participants. That is, k out of n participants also act as dealers. Meanwhile, the scheme achieves two structures simultaneously: the threshold structure and the adversary structure. The former means that t or more than t participants can retrieve the master secret, and the latter one means that there are some subsets containing at least t participants cannot recover the secret. In addition, the scheme uses the property of additive homomorphism in the reconstruction phase for reducing the storage cost. Therefore, the size of share kept by each participant is bounded by $\frac{2|S|}{t}$.

Our scheme satisfies confidentiality in the sense that any unauthorized subset of participants cannot recover the shared secret. It can be shown that all sub-shares of the scheme are strong t-consistent, thus the proposed scheme can prevent any malicious participants from cheating. In particular, most VSSSs [6-7,28] only support post-verification property that each participant submits his secret share for doing reciprocal verifications. Therefore, the colluded participants (CPs) can obtain real shares of other participants but provide false shares for cheating others. Then, an unauthorized subset of CPs may recover the secret. Our scheme achieves pre-verification property, where all participants only need to publish their verification shares in the verification process, without revealing any information about the real master shares. Thus, the new proposal can prevent the attack from CPs. Finally, we compare our proposal with the previous (n,t,n) SSSs [11,17,22] from the perspectives of what kinds of access structures they achieve, what kinds of functionalities they support and whether heavy

storage cost for secret share is required. Then it shows that our scheme takes the following advantages: (a) achieving the adversary structure, (b) allowing any k out of n participants to operate as dealers, (c) small sized secret share.

The rest of this work is arranged as follows: In Section 2, some basic concepts are reviewed. Our scheme is presented in Section 3. Section 4 proves the confidentiality, verification and reconstruction properties of the newly proposed schemes. Finally, conclusions are provided in Section 5.

2. Preliminaries

In this section, we review some basic concepts.

2.1 Strong VSSS

Definition 1. Strong t-consistent[11]. In a (t,n) secret sharing scheme, the n shares are strong t-consistent if (a) any subset containing t or more than t participants can determine the same secret; (b) any $t-1$ shares cannot determine the same secret.

Definition 2. Strong VSSS[11]. In a strong verifiable secret sharing scheme, each participant can verify that the shares used for recovering the secret are strong t-consistent.

2.2 The access structure and the adversary structure

Let $Q=\{P_1,P_2,\ldots,P_n\}$ be the set of participants. An access structure [24], denoted by Γ, is a collection of subsets of Q satisfying the monotone ascending property: for any $A'\in\Gamma$ and $A\in 2^Q$, $A\supseteq A'$ implies $A\in\Gamma$. An adversary structure [24], named as Ω, is a collection of subsets of Q satisfying the monotone descending property: for any $A'\in\Omega$ and $A\in 2^Q$, $A\subseteq A'$ implies $A\in\Omega$. Because of the monotone properties, for any access structure Γ and any adversary structure Ω, it is enough to consider the minimum access structure:

$$\Gamma_{min}=\{A\in\Gamma \mid \forall B\subset A\Rightarrow B\notin\Gamma\} \tag{1}$$

and the maximum adversary structure:

$$\Omega_{\max}=\{B\in\Omega \mid \forall A\supset B\Rightarrow A\notin\Omega\}. \tag{2}$$

3. Our scheme

In this section, we propose a strong (k,t,n) verifiable multi-secret sharing scheme that achieves both the threshold and the adversary structure.

3.1 The initialization phase

Let $Q=\{P_1,P_2,\ldots,P_n\}$ denote the set of n participants, and S denote the master secret. Let $Q_0=\{P_1,P_2,\ldots,P_k\}$ be the set of k dealers ($k\le n$ and $Q_0\subseteq Q$). Suppose that $A_1,A_2,\ldots,A_m$ are m subsets contained in $\Omega_{\max}$ and each of them has at least t participants. Now, we can define the access structure of our scheme as follows:

$$\Gamma = \{X :| X |\geq t \text{ and } X \not\subseteq A_j,\ j = 1,\cdots,m\}. \quad (3)$$

That are, (a) if $| X |\geq t$ and $X \not\subseteq A_j$ $(\mathrm{j} = 1,2,\cdots,\mathrm{m})$, then participants in set X can reconstruct the master secret S; (b) if $| X |< t$ or $X \subseteq A_j$ $(1 \leq j \leq m)$, then the participants in X cannot reconstruct S.

3.2 Distribution and Reconstruction of secrets

Let F_p be a finite field, where p is a large prime. Based on the previous (n,t,n) schemes [17], the new scheme presents a more general model that any k out of n participants also operate as dealers without the assistance of a mutually trusted third party. The master secrets are the summations of threshold parameters and adversary control parameters. Then, each step of the construction is accomplished by two parallel algorithms for the threshold and the adversary structure: the threshold structure algorithm is based on Shamir's secret sharing algorithm to create m master shares, and the adversary structure algorithm is used to generate control shares. Now, the distribution and reconstruction phases are described as follows:

Step 1. Master secret generation

Each participant P_α $(1 \leq \alpha \leq k)$ constructs a polynomial

$$f_\alpha(x) = S_{\alpha,0} + S_{\alpha,1}x + \cdots + S_{\alpha,t-1}x^{t-1},$$

where $S_{\alpha,l}$ $(S_{\alpha,l} \in F_p^m,\ 0 \leq l \leq t-1)$ is an m-dimensional column vector. The master polynomial with respect to the threshold structure is defined by

$$F(x) = \sum_{\alpha=1}^{k} f_\alpha(x).$$

Let $K = [S_0, S_1, \cdots, S_{t-1}]$ be an $m \times t$ matrix, where

$$S_l = \sum_{\alpha=1}^{k} S_{\alpha,l}$$

for $l = 0,1,\cdots,t-1$. On the other hand, P_α $(1 \leq \alpha \leq k)$ selects an element D_α from F_p. The control parameter for the adversary structure is defined by

$$D = \sum_{\alpha=1}^{k} D_\alpha.$$

Let M be an $m \times t$ matrix with all elements being D. Then the master secret S can be determined as

$$S = K + M.$$

Step 2. Sub-share generation

To the threshold structure, each participant P_α $(1 \leq \alpha \leq k)$ uses Shamir's distribution algorithm to generate sub-shares, $s_{\alpha,i} = f_\alpha(x_i)$ $(i = 1,\cdots,n)$, for other participants. Here, $s_{\alpha,i}$ is also an m-dimensional column vector. Then P_α sends $s_{\alpha,i}$ to P_i secretly, and each participant P_i $(1 \leq i \leq n)$ will receive k sub-shares $s_{\alpha,i}$, for $\alpha = 1,\cdots,k$.

In order to realize the adversary structure, each participant P_α creates an adversary control coalition $H_\alpha = \{d_{\alpha,1}, d_{\alpha,2}, \cdots, d_{\alpha,m}\}$ $(d_{\alpha,j} \in F_p,\ 1 \leq \alpha \leq k$ and $1 \leq j \leq m)$ such that

$$D_\alpha = d_{\alpha,1} + d_{\alpha,2} + \ldots + d_{\alpha,m}.$$

If $P_i \in A_j$ $(1 \le j \le m)$, then P_α deletes $d_{\alpha,j}$ from H_α, and sends the remaining elements in H_α to P_i, for $i = 1, \cdots, n$. Each participant P_i $(1 \le i \le n)$ obtains k coalitions $H_\alpha \setminus \{d_{\alpha,j} \mid P_i \in A_j,\ j = 1, \cdots, m\}$ from participant P_α, for $\alpha = 1, \cdots, k$.

Step 3. Master share generation

Each participant P_i computes one m-dimensional threshold share and m_i adversary control shares. P_i calculates threshold master share

$$s_i = \sum_{\alpha=1}^{k} s_{\alpha,i} = \sum_{\alpha=1}^{k} f_\alpha(x_i).$$

Meanwhile, participant P_i combines the received sub-shares into the corresponding adversary control share as

$$d_j = \sum_{\alpha=1}^{k} d_{\alpha,j}, \text{ for } j = 1, \cdots, m,$$

Then, he keeps a coalition

$$H^{(i)} = \{d_j \mid P_i \notin A_j,\ j = 1, \cdots, m\}.$$

That is, $|H^{(i)}| = m_i$, and $m_i \le m$.

Step 4. Verification phase

Using the method of verification in Liu SSS [11], all participants perform together for selecting a k-tuple weight vector $\vec{w} = (w_1, w_2, \ldots, w_k)$, such that $\vec{w}$ is linearly independent to vector $(1, 1, \cdots, 1)$, where $w_l \in F_p$ ($l = 1, \cdots, k$). Then, P_i $(1 \le i \le n)$ computes and broadcasts his verification share v_i as

$$v_i = \sum_{\alpha=1}^{k} w_\alpha \cdot s_{\alpha,i}.$$

Any t participants use Lagrange interpolation formula on the published verification shares. If the verification polynomial

$$F_w(x) = \sum_{\alpha=1}^{k} w_\alpha \cdot f_\alpha(x)$$

is t-1 exactly, then the master shares are strong t-consistent (Theorem 2 and Lemma 3). Actually, the verification property is pre-verifiable.

Step 5. Master secret reconstruction

For any authorized subset $X \in \Gamma$ ($|X| \ge t$), the participants in X obtain d_j $(j = 1, 2, \ldots, m)$. With the help of the property of additive homomorphism, they compute

$$D = \sum_{\alpha=1}^{k} D_\alpha = \sum_{j=1}^{m} d_j$$

for reconstructing the adversary control parameter. Meanwhile, with the knowledge of any t master shares with respect to the threshold structure, matrix S^* can be recovered by Lagrange interpolation formula (denoted by $F_X(\cdot)$). That is, the master polynomial is

$$F(x) = \sum_{\alpha=1}^{k} f_\alpha(x) = F_X(s_{l_1}, s_{l_2}, \cdots, s_{l_t}),$$

where $s_{l_1},\ldots,s_{l_t}$ are threshold shares. Thus, the master secret matrix S as $S=K+M$ can be reconstructed by the participants in X (see the correctness proof of Theorem 4).

Now, we analyze the aforementioned distribution and the reconstruction phases. Each participant P_i computes his adversary shares as $d_j=\sum_{\alpha=1}^{k} d_{\alpha,j}$, for $j=1,\cdots,m$ and $P_i\notin A_j$, without storing all received sub-shares $d_{\alpha,j}(\alpha=1,\cdots,k,\ j=1,\cdots,m)$. Otherwise, the number of shares kept by each participant is proportional to the number of participants. Observe that the reconstruction of control parameter D is achieved based on the property of additive homomorphism. The following two tables present the distribution of master shares of the scheme.

Table 1. Master share for threshold structure

	P_1	$\cdots$	P_k	**Master share**
P_1	$s_{1,1}$	$\cdots$	$s_{k,1}$	$s_1=\sum_{\alpha=1}^{k} s_{\alpha,1}$
P_2	$s_{1,2}$	$\cdots$	$s_{k,2}$	$s_2=\sum_{\alpha=1}^{k} s_{\alpha,2}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
P_n	$s_{1,n}$	$\cdots$	$s_{k,n}$	$s_n=\sum_{\alpha=1}^{k} s_{\alpha,n}$

Table 2. Master share for adversary structure

	P_1	$\cdots$	P_k	**Master share**
P_1	$H_1\setminus\{d_{1,j}\mid P_1\in A_j\}$	$\cdots$	$H_k\setminus\{d_{k,j}\mid P_1\in A_j\}$	$\{d_j\mid P_1\notin A_j,1\le j\le m\}$
P_2	$H_1\setminus\{d_{1,j}\mid P_2\in A_j\}$	$\cdots$	$H_k\setminus\{d_{k,j}\mid P_2\in A_j\}$	$\{d_j\mid P_2\notin A_j,1\le j\le m\}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
P_n	$H_1\setminus\{d_{1,j}\mid P_n\in A_j\}$	$\cdots$	$H_k\setminus\{d_{k,j}\mid P_n\in A_j\}$	$\{d_j\mid P_n\notin A_j,1\le j\le m\}$

4. Analysis and discussion

In the upcoming section, we present the analysis of our proposed scheme.

4.1 Security Proof

The security of secret sharing scheme is based on that of Shamir's SSS, thus the proposal is secure in information theory. Now we prove that any unauthorized subset cannot recover the shared secret (Theorem 1).

Theorem 1. If $|X|<t$ or $X\subseteq A_j(1\le j\le m)$, then the participants in set X cannot

reconstruct the master secret matrix S.

Proof. If $|X|<t$, the participants cannot get enough threshold shares to generate $(t-1)$-degree master polynomial $F(x)$. Furthermore, the vector $\vec{w}=(w_1,w_2,\cdots,w_k)$ is linearly independent to $(1,1,\cdots,1)$, this implies that the verification shares cannot reveal any information about master shares. Thus, they cannot compute matrix K. On the other hand, if $X \subseteq A_j$ $(1\le j\le m)$, any participant in X is not able to obtain the array $\{d_{1,j},d_{2,j},\cdots,d_{k,j}\}$, then $d_j=\sum_{\alpha=1}^{k} d_{\alpha,j}$ and thus, D cannot be computed. Therefore, the participants in X cannot recover the master secret matrix S.

4.2 The Verification property

The scheme satisfies the pre-verification property that any t participants can check the validity of secret shares without disclosing their real share. Now we give the verification analysis below.

Theorem 2. Any t or more than t participants can retrieve verification polynomial $F_w(x)$.

Proof. With the knowledge of any t or more than t verification shares, the participants can recover verification polynomial $F_w(x)=\sum_{\alpha=1}^{k} w_\alpha f_\alpha(x)$ with the help of the property of additive homomorphism and applying Lagrange interpolation formula on the verification shares. Let $X=\{P_{l_1},P_{l_2},\cdots,P_{l_t}\}$ be an authorized subset of participants, and

$$F_X(s_{\alpha,l_1},s_{\alpha,l_2},\cdots,s_{\alpha,l_t})=\sum_{d=1}^{t} s_{\alpha,l_d}\cdot\prod_{1\le r\le t,r\ne d}\frac{x-x_{l_r}}{x_{l_d}-x_{l_r}},$$

where $y_{l_d}=\prod_{1\le r\le t,r\ne d}\frac{x-x_{l_r}}{x_{l_d}-x_{l_r}}$ $(d=1,\cdots,t)$ are called interpolation coefficients. Then, we obtain the following equations:

$$\begin{aligned} f_1(x)&=F_X(s_{1,l_1},s_{1,l_2},\cdots,s_{1,l_t});\\ f_2(x)&=F_X(s_{2,l_1},s_{2,l_2},\cdots,s_{2,l_t});\\ &\cdots\\ f_k(x)&=F_X(s_{k,l_1},s_{k,l_2},\cdots,s_{k,l_t}). \end{aligned}$$

Thus, we have

$$\begin{aligned} F_w(x)&=\sum_{\alpha=1}^{k} w_\alpha\cdot f_\alpha(x) && (4)\\ &=w_1F_X(s_{1,l_1},s_{1,l_2},\cdots,s_{1,l_t})+\cdots+w_kF_X(s_{k,l_1},s_{k,l_2},\cdots,s_{k,l_t}) && (5)\\ &=F_X[(\sum_{\alpha=1}^{k} w_\alpha\cdot s_{\alpha,l_1}),(\sum_{\alpha=1}^{k} w_\alpha\cdot s_{\alpha,l_2}),\cdots,(\sum_{\alpha=1}^{k} w_\alpha\cdot s_{\alpha,l_t})] && (6)\\ &=F_X(v_{l_1},v_{l_2},\cdots,v_{l_t}) && (7) \end{aligned}$$

We observe that Eq.(5) and Eq.(6) follow from Shamir's secret reconstruction algorithm using Lagrange interpolation formula and the property of additive homomorphism, respectively.

Lemma 3. If the degree of verification polynomial $F_w(x)=\sum_{\alpha=1}^{k} w_\alpha\cdot f_\alpha(x)$ is exactly $t-1$, then, the degree of master polynomial $F(x)=\sum_{\alpha=1}^{k} f_\alpha(x)$ is exactly $t-1$.

Proof. We follow the same method for proving this lemma as used for proving Theorem 1 in [17]. Assume that there exists a polynomial $f_\alpha(x)(1\le\alpha\le k)$, with degree larger than $t-1$ (say t). Let a_α be the first coordinate of the coefficient vector associated with the term x^t of $f_\alpha(x)$. Then, the probability that the degree of verification polynomial $F_w(x)=\sum_{\alpha=1}^{k} w_\alpha\cdot f_\alpha(x)$ is $t-1$ exactly equals to the probability that $w_1a_1+w_2a_2+\ldots+w_ka_k=0$. Since a_α $(a_\alpha\in F_p^m,\ 1\le\alpha\le k)$ is selected randomly and independently, then this probability is $\frac{(p^m)^{n-1}}{(p^m)^n}=\frac{1}{p^m}$, which can be ignored, for large prime p. Thus, if the degree of polynomial $F_w(x)$ is exactly $t-1$, then the degree of each polynomial $f_\alpha(x)$ $(1\le\alpha\le k)$ is at most $t-1$.

On the other hand, let $a_\alpha^{'}$ be the first coordinate of the coefficient vector associated with the term x^{t-1} of $f_\alpha(x)$. If at least one of $a_\alpha^{'}(1\le\alpha\le k)$ is nonzero, then the probability that $a_1^{'}+a_2^{'}+\ldots+a_k^{'}=0$ is $\frac{1}{p^m}$, which can also be negligible. Therefore, the degree of the master polynomial $F(x)=\sum_{\alpha=1}^{k} f_\alpha(x)$ is exactly $t-1$.

From the aforementioned proof, we conclude that if colluded participants in Q_0 select polynomials $f_\alpha(x)(1\le\alpha\le k)$, having degree not equal to $t-1$, then they cannot pass the verification. Therefore, the proposed scheme satisfies the definition of strong VSSS. Meanwhile, since the vector $(w_1,\cdots,w_k)$ is linearly independent to vector $(1,\cdots,1)$, hence no information about the real master shares can be revealed in the verification phase. Thus, the scheme has the advantage of pre-verification for that any participant doesn't need to submit his real share in the verification phase. Moreover, it is worthwhile to note that the fraud probability of the new scheme is $\frac{1}{p^m}$. This probability takes an exponential decline increment in the value of parameter m. Therefore, compared with the previous VSSS [17] having the fraud probability $\frac{1}{p}$, our scheme just needs a smaller p for insuring that the corresponding fraud probability can be negligible. In such a way, the computational efficiency is improved to some extent.

4.3 The Reconstruction property

Theorem 4. For any authorized subset $X\in\Gamma$, the participants in X can reconstruct the master secret S.

Proof. Let $(w_1,w_2,\cdots,w_k)=(1,1,\cdots,1)$ in the proof of Theorem 2, then we have that the participants in X can reconstruct master polynomial

$$F(x)=\sum_{\alpha=1}^{k} f_\alpha(x)=F_X(s_{l_1},\cdots,s_{l_t}).$$

to obtain matrix K. On the other hand, since $X\in\Gamma$, that is, $|X|\ge t$ and $X\not\subseteq A_j(j=1,2,\cdots,m)$, this implies that there exists at least one participant having $d_j=\sum_{\alpha=1}^{k} d_{\alpha,j}$, for every $j\in\{1,2,\cdots,m\}$. Then the participants in X can obtain set

$\{d_1, d_2, \cdots, d_m\}$ by pooling together their shares. Furthermore, we have that

$$\sum_{j=1}^{m} d_j = \sum_{j=1}^{m} (\sum_{\alpha=1}^{k} d_{\alpha,j}) = \sum_{\alpha=1}^{k} (\sum_{j=1}^{m} d_{\alpha,j}) = \sum_{\alpha=1}^{k} D_\alpha = D.$$

The second equation follows from the property of additive homomorphism. Thus, all the participants in X work together for computing $D = \sum_{j=1}^{m} d_j$ and get matrix M. Hence, they can recover the master secret matrix S.

4.4 The Dynamic property

A secret sharing scheme is said to be dynamic, if any participant can join and leave dynamically. The previous (n,t,n) threshold SSSs [11,17] realize the dynamic property. Now we point out that our scheme under the complicated model also supports this property and analyze various cases in terms of control parameter D for the adversary structure.

Case 1. Suppose that participant P_l leaves from set $\{P_1, \ldots, P_n\}$. If $P_l \in Q_0$, then control parameter D of the scheme is determined as

$$D = \sum_{\alpha=1}^{l-1} D_\alpha + \sum_{\alpha=l+1}^{k} D_\alpha.$$

Participant P_i $(1 \le i \le n,\ i \ne l)$ just needs to delete set $H_l \setminus \{d_{l,j} \mid P_i \in A_j,\ j = 1, \cdots, m\}$ received from P_l. The remaining participants compute their new shares as

$$d_j = \sum_{\alpha=1}^{l-1} d_{\alpha,j} + \sum_{\alpha=l+1}^{k} d_{\alpha,j} \quad (j = 1, \cdots, m).$$

If $P_l \in Q \setminus Q_0$, then k dealers need to update their control parameters $d_{\alpha,j}$, for $\alpha = 1, \cdots, k$, and $P_l \notin A_j$. The participants compute their new shares as

$$d_j = \sum_{\alpha=1}^{k} d_{\alpha,j}, \text{ for } j = 1, \cdots, m.$$

Case 2. Suppose that a new participant P_{n+1} joins. If P_{n+1} contained in Q_0 acts as a dealer, then, he is required to choose one element $D_{n+1} (\in F_p)$ and generate a control coalition $H_{n+1} = \{d_{n+1,1}, d_{n+1,2}, \cdots, d_{n+1,m}\}$ such that $D_{n+1} = \sum_{j=1}^{m} d_{n+1,j}$. Then, the control parameter D is determined as

$$D = \sum_{\alpha=1}^{k} D_\alpha + D_{n+1}.$$

P_{n+1} sends $H_{n+1} \setminus \{d_{n+1,j} \mid P_i \in A_j,\ j = 1, \cdots, m\}$ to participant $P_i (1 \le i \le n)$. Similarly, participant $P_\alpha (1 \le \alpha \le k)$ needs to send $H_\alpha \setminus \{d_{\alpha,j} \mid P_{n+1} \in A_j,\ j = 1, \cdots, m\}$ to P_{n+1}. All participants compute their new shares as

$$d_j = \sum_{\alpha=1}^{k} d_{\alpha,j} + d_{n+1,j} \quad (j = 1, \cdots, m).$$

If $P_{n+1} \notin Q_0$, then he receives $H_\alpha \setminus \{d_{\alpha,j} \mid P_{n+1} \in A_j,\ j = 1, \cdots, m\}$ from $P_\alpha (1 \le \alpha \le k)$ and computes $d_j = \sum_{\alpha=1}^{k} d_{\alpha,j}$.

The analysis on threshold parameter K can be discussed in the same way.

4.5 Efficiency analysis

In this section, we analyze the efficiency of the newly proposed scheme from angles of computational complexity and communication cost, respectively.

With respect to the computation complexity, we mainly count the number of polynomial evaluation and polynomial interpolation in three stages:

- **Sharing phase:** Each participant P_α $(1 \le \alpha \le k)$ computes $s_{\alpha,i} = f_\alpha(x_i)$ $(i = 1, \cdots, n)$ and sends $s_{\alpha,i}$ to P_i, where $s_{\alpha,i}$ is an m-dimensional column vector. Thus, mnk polynomial evaluations are needed.
- **Verification phase:** Each participant P_i $(1 \le i \le n)$ computes an m-dimensional verification share $v_i = \sum_{\alpha=1}^{k} w_\alpha \cdot s_{\alpha,i}$. The operation of the form of $\sum_{\alpha=1}^{k} w_\alpha \cdot s_{\alpha,i}$ can be viewed as a polynomial evaluation. Thus, mn polynomial interpolations should be used. Besides, t participants adopt Lagrange polynomial interpolation on the published verification shares. Thus, m polynomial interpolations are needed.
- **Reconstruction phase:** Based on Lagrange interpolation formula, the secret verification and reconstruction can be completed by computing the same interpolating coefficients y_{l_d} $(d = 1, \cdots, t)$. Thus, the reconstruction phase only needs m polynomial evaluations.

Table 3. Computational complexity

	Polynomial evaluation	Polynomial interpolating
Sharing phase	mnk	–
Verification phase	mn	m
Reconstruction phase	m	–

Remark. The above analysis on computational complexity is aimed at the threshold structure. In addition, since the realization of the adversary structure only utilizes simple module additions, therefore, the operation of this part can be negligible.

With respect to the communication cost, we describe the bits of communication cost for the threshold and the adversary structure:

- Access structure: P_α $(1 \le \alpha \le k)$ sends m-dimensional column vector $s_{\alpha,i}$ to $P_i (1 \le i \le n)$. Thus, this part of communication costs $mnk \cdot \log p$ bits.
- Adversary structure: Each participant $P_\alpha (1 \le \alpha \le k)$ sends $H_\alpha \setminus \{d_{\alpha,j} \mid P_{n+1} \in A_j,\ j = 1, \cdots, m\}$ to $P_i (1 \le i \le n)$. Since $\left| H_\alpha \setminus \{d_{\alpha,j} \mid P_{n+1} \in A_j,\ j = 1, \cdots, m\} \right| \le m$, then this part of communication cost is bounded by $mnk \cdot \log p$ bits.

Table 4. Communication cost

	Threshold structure	Adversary structure
Bit number	$mnk \cdot \log p$	$mnk \cdot \log p$

4.6 Information rate

The information rate [18] of one secret sharing scheme is defined by

$$\rho = \frac{|S|}{max|S(P_i)|},$$

where $|S|$ denotes the size of secret, and $|S(P_i)|$ is the size of share kept by participant P_i.

In the scheme, we have that

$$\rho = \frac{|S|}{max|S(P_i)|} = \frac{(m \times t) \cdot \log p}{(m + max(m_i)) \cdot \log p},$$

Since $t \geq 2$ and $m > max(m_i)$, then $\rho > \frac{t}{2}$ and $\rho > 1$. Meanwhile, we can obverse that the size of share kept by each participant is bounded by $\frac{2|S|}{t}$. In Zhao's scheme, the size of share is $\frac{|S|+|a|}{t} + \frac{(|S|+|a|)(m-1)}{t^2}$ [28]. For convenience, let $|a|$, the size of populated data, be zero, then the corresponding information rate is given by $\frac{t^2}{t+m-1}$ $(1 \leq m < \sum_{i=t}^{n} C_n^i)$. The two schemes have equal information rates, that is, $\frac{t}{2} = \frac{t^2}{t+m-1}$, then $m = t+1$. Then, we have that Zhao's SSS has a higher information rate if $m \leq t$; our scheme is superior to Zhao's SSS if $m \geq t+1$. Considering the computational complexity of Lagrange interpolation in a threshold SSS, the designer normally selects a small integer as the threshold value. That is, in the most cases, $m \geq t+1$ holds and our scheme has higher information rate than Zhao's SSS.

Finally, the performance comparison among SSSs of [17,28] and our proposal is demonstrated as follows:

Table 5. Performance comparison

	Liu SSS [17]	**Zhao SSS [28]**	**Our SSS**
basic model	(n,t,n) VSSS	(t,n) VSSS	(k,t,n) VSSS
Threshold structure	Yes	Yes	Yes
Adversary structure	No	Yes	Yes
Without TTPs	Yes	No	Yes
Without modular Exp computation	Yes	No	Yes
Share size	$\|S\|$	$\frac{(t+m-1)\|S\|}{t^2}$	$\frac{2\|S\|}{t}$
Information rate	$\rho = 1$	$\rho = \frac{t^2}{t+m-1}$	$\rho > \frac{t}{2}$
Pre-verification property	Yes	No	Yes
Infor. Theory security	Yes	No	Yes

The comparisons given in **Table 5** can be further depicted in **Fig. 1** and **Fig. 2**. In **Fig. 1** we compare our proposal with the schemes given in [28] and [17] from the perspectives of what kinds of functionalities they support, which kind of security they achieve, and whether the trusted third party and some complex computation (such as modular exponential) are required. From Figure 1, we can see that our proposal covers all these six desirable merits: Simultaneously supporting adversary structure, threshold structure and pre-verification, achieving information-theory security (or equivalently, without depend upon any intractability assumption), and needless TTP and modular exponential computation. In Figure 2 we compare these schemes from the perspective of information rate. It shows that our scheme can gain even higher information rate. In particular, with the increase of m (i.e., the number of adversary sets) or t (i.e., the threshold value), the advantages of our proposal become even clear.

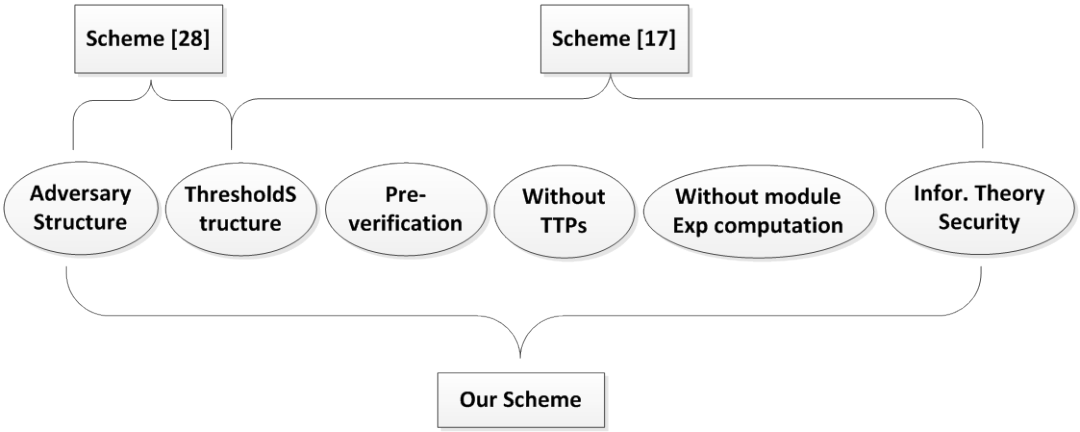

Fig. 1. Functionalities comparison

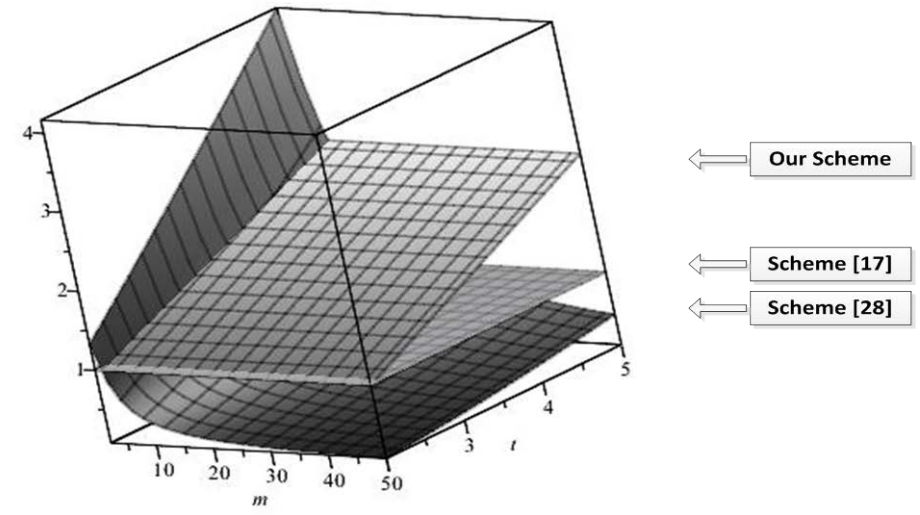

Fig. 2. Information rate comparison

Remark. Our scheme has relatively higher computational complexity and communication cost among the three schemes, since it achieves more properties than scheme [17] and scheme [28], respectively.

5. Conclusions

In this paper, based on the previous (n,t,n) VSSSs, we propose a more general (k,t,n) VSSS, in which any k out of n participants also operate as dealers. The scheme realizes the threshold and the adversary structure simultaneously. In such a way, it restricts the powers of participants in secret reconstruction phase efficiently. Taking the advantage of additive homomorphism, the size of share stored by each participant is reduced for improving the efficiency of our scheme. In addition, our scheme has the advantage of the pre-verification property.

References

[1] S. Agrawal, "Verifiable secret sharing in a total of three rounds," *Information Processing Letters*, 112, pp. 856-859, 2012. Article (CrossRef Link)

[2] J.C. Benaloh, "Secret sharing homomorphisms: keeping shares of a secret. CRYPTO," *Lecture Notes in Computer Science*, 263, pp. 251-260, Springer, 1986. Artical (CrossRef Link)

[3] J.C. Benaloh, J. Leichter, "Generalized Secret Sharing and Monotone Functions," *CRYPTO'88, Lecture Notes in Computer Science*, 403, pp. 27-35, Springer, 1990. Article(CrossRef Link)

[4] G.R. Blakley, "Safeguarding cryptographic keys," in *Proc. of AFIPS 1979 National Computer Conference*, pp. 313-317, June, 1979. Artical (CrossRef Link)

[5] H. Y. Chien, J.K. Jan, Y.M. Tseng, "A practical (t,n) multi-secret sharing scheme," *IEICE Transactions on Communications/Electronics/Information and Systems*, pp. 2762−2765, 2000. Artical (CrossRef Link)

[6] M.H. Dehkordi, S. Mashhadi, "An efficient threshold verifiable multi-secret sharing," *Computer Standards & Interfaces*, 30, pp. 187-190, 2008. Article (CrossRef Link)

[7] M.H. Dehkordi, S. Mashhadi, "New efficient and practical verifiable multi-secret sharing schemes," *Information Sciences*, 178, pp. 2262-2274, 2008. Article (CrossRef Link)

[8] C. Guo, C.C. Chang, C. Qin, "A hierarchical threshold secret image sharing," *Pattern Recognition Letters*, 33, pp. 83-91, 2012. Article (CrossRef Link)

[9] Y.B. Guo, J.F. Ma, "Practical secret sharing scheme realizing generalized adversary structure," *Journal of Computer Science and Technology*, 19, pp. 564-569, 2004. Article (CrossRef Link)

[10] L. Harn, M. Fuyou, "Multilevel threshold secret sharing based on the Chinese Remainder Theorem," *Information Processing Letters*, 114, pp. 504-509, 2014. Article (CrossRef Link)

[11] L. Harn, C. Lin, "Strong (n,t,n) verifiable secret sharing scheme," *Information Sciences*, 180, pp. 3059-3064, 2010. Article (CrossRef Link)

[12] S. Iftene, "General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting," *Electronic Notes in Theoretical Computer Science*, 186, pp. 67-84, 2007. Article (CrossRef Link)

[13] Ingemarsson, Simmons, "A Protocol to Set Up Shared Secret Schemes without the Assistance of a Mutually Trusted Party," *Advances in Cryptology: Proceedings of EUROCRYPT*, 1990. Artical (CrossRef Link)

[14] M. Ito, A. Saito, T. Nishizeki, "Secret sharing scheme realizing general access structure," in *Proc. of IEEE Global Telecommunications Conference-GLOBECOM'87*, pp. 99-102, 1987. Artical (CrossRef Link)

[15] Q. Li, D.Y. Long, W.H. Chan, D.W.Qiu, "Sharing a quantum secret without a trusted party," URL. Article(CrossRef Link)

[16] T.Y. Lin, T.C. Wu, "(t, n) threshold verifiable multisecret sharing scheme based on factorisation intractability and discrete logarithm module a composite problems," *IEE Proceedings on Computers and Digital Techniques*, 146, pp. 264-268, 1999. Article (CrossRef Link)
[17] Y.X. Liu, L. Harn, C.N. Yang, Y.Q. Zhang, "Efficient (n,t,n) secret sharing schemes," *Journal of Systems and Software*, 85, pp. 1325-1332, 2012. Article (CrossRef Link)
[18] C. Padro, G. Saez, "Lower bounds on the information rate of secret sharing schemes with homogeneous access structure," *Information Processing Letters*, 83, pp. 345-351, 2002. Article (CrossRef Link)
[19] N. Pakniat, M. Noroozi, Z. Eslami, "Secret image sharing scheme with hierarchical threshold access structure," *Journal of Visual Communication and Image Representation*, 25, pp. 1093-1101, 2014. Article (CrossRef Link)
[20] A. Parakh, S. Kak, "Space efficient secret sharing for implicit data security," *Information Sciences*, 181, pp. 335-341, 2011. Article (CrossRef Link)
[21] A. Patra, A. Choudhary, T. Rabin, C.P. Rangan, "The Round Complexity of Verifiable Secret Sharing Revisited. CRYPTO," *Lecture Notes in Computer Science*, 5677, pp. 487-504, Springer, 2009. Artical (CrossRef Link)
[22] T.P. Pedersen, "A threshold cryptosystem without a trusted party," *in Proc. of the Eurocrypt'91*, *Lecture Notes in Computer Science*, 547, pp. 522-526, Springer, 1991. Artical (CrossRef Link)
[23] H.W. Qin, Y.W. Dai, Z.Q. Wang, "A secret sharing scheme based on (t,n) threshold and adversary structure," *International Journal of Information Security*, 8, pp. 379-385, 2009. Article(CrossRef Link)
[24] A. Shamir, "How to share a secret," *Communications of the ACM*, 22, pp. 612-613, 1979. Article(CrossRef Link)
[25] R.H. Shi, L.S. Huang, Z. Hong, "An Efficient (t, n)-Threshold Multi-Secret Sharing Scheme," in *Proc. of International Conference on Networks & Soft Computing*, pp. 580-583, 2008. Artical (CrossRef Link)
[26] G.L. Wang, S. Qing, "A Threshold Undeniable Signature Scheme without a Trusted Party," *Journal of Software*, 13, pp. 1757-1764, 2002. Artical (CrossRef Link)
[27] C.C. Yang, T.Y. Chang, M.S. Hwang, "A (t,n) multi-secret sharing scheme," *Applied Mathematics and Computation*, 151, pp. 483−490, 2004. Article (CrossRef Link)
[28] D.W. Zhao, H.P. Peng, C. Wang, Y.X. Yang, "A secret sharing scheme with a short share realizing the (t,n) threshold and the adversary structure," *Computers and Mathematics with Applications*, 64, pp. 611-615, 2012. Article (CrossRef Link)

Jing Li received the B.S. degree from Inner Mongol Normal University in 2010 an d the M.S. degree from Shananxi Normal University in 2013. Her current research in terests include modern cryptography, network security, finite field and its application s, etc. She is a doctoral candidate studying in Beijing University of Posts and Teleco mmunications.

Licheng Wang received the B.S. degree from Northwest Normal University in 199 5, the M.S. degree from Nanjing University in 2001, and the PhD degree from Shang hai Jiao Tong University in 2007. His current research interests include modern crypt ography, network security, trust management, etc. He is an associate professor in Bei jing University of Posts and Telecommunications.

Jianhua Yan received the B.S. degree B.S. degree from JiLin University in 2002, the M.S. degree from LiaoNing University of Petro-Chemical Technology in 2005. His current research interests include lattice-based cryptosystem and information security. Now he is a doctoral candidate studying in Beijing University of Posts and Telecommunications.

Xinxin Niu is an professor of Computer Science and Technology at Beijing University of Posts and Telecommunications. She received the MS degree from Beijing University of Posts and Telecommunications in 1988, the PhD degree from Chinese University of Hong Kong in 1997. Her current research interests include network security, digital watermarking and digital rights management, etc.

Yixian Yang is a Professor of Computer Science and Technology at Beijing University of Posts and Telecommunications and also the director of the National Engineering Laboratory for Disaster Backup and Recovery of China. He is a fellow of China Institute of Communications (CIC), and a council member of Chinese Institute of Electronics (CIE) and Chinese Association for Cryptologic Research (CACR). He is the editor in chief of Journal on Communications of China. He received his MS degree in Applied Mathematics and PhD degree in Signal and Information Processing from Beijing University of Posts and Telecommunications in 1986 and 1988, respectively. His research interests include coding theory and cryptography, information security and network security, disaster backup and recovery, signal and information processing, etc.