Cryptogr. Commun. (2017) 9:625–635
DOI 10.1007/s12095-016-0205-6

# Secret sharing schemes for compartmented access structures

Xianfang Wang[1] · Can Xiang[2,3] · Fang-Wei Fu[1]

Received: 12 April 2016 / Accepted: 14 September 2016 / Published online: 20 September 2016

**Abstract** In this paper, we devise ideal and probabilistic secret sharing schemes for two kinds of compartmented access structures. The first one is a compartmented access structures with hierarchical compartments. The second one is the compartmented access structures with strictly lower bounds. We propose ideal and probabilistic schemes for these two compartmented access structures by using the idea of bivariate interpolation.

**Keywords** Secret sharing schemes · Compartmented access structures · Ideality · Bivariate interpolation

**Mathematics Subject Classification (2010)** 94A62 · 94A60

## 1 Introduction

Secret sharing schemes (SSSs) were introduced independently by Shamir [13] and Blakley [1]. A secret sharing scheme (SSS) is a method that a *dealer* distributes shares of a secret

✉ Can Xiang
cxiangcxiang@hotmail.com

Xianfang Wang
xianfw@mail.nankai.edu.cn

Fang-Wei Fu
fwfu@nankai.edu.cn

[1] Chern Institute of Mathematics and LPMC, Nankai University, Tianjin, 300071,
People's Republic of China

[2] College of Mathematics and Informatics, South China Agricultural University, Guangzhou,
510642, People's Republic of China

[3] Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang
Technological University, Singapore 637371, Singapore

to participants such that only *authorized* subsets of participants can recover the secret from their shares. Shamir's scheme is called $(t, n)$ *threshold* SSS. In the scheme, the authorized set is the set that contains $t$ or more participants. The threshold scheme was generalized to ones with *access structure (AS)*. Although there exists a linear SSS for every AS [4, 11], but the known general constructions are impractical because the size of the shares is exponential. Since the seminal work of Shamir, many applications of SSS to several different kinds of cryptographic protocols have appeared. For instance, SSS can be used in multiparty computation and secure key management schemes. The relation between SSS and linear code has also been studied for a long time(set [5–8] for example). SSS plays an important role in cryptography. So, it is interesting to devise efficient and practical schemes for different kinds of access structures. For further introductions to secret sharing, the interested readers can refer to [3, 15] and the references therein. The definitions of the ASs appeared in this section will be given in Section 2.

We focused on compartmented AS in this work. Let us suppose the ASs are monotone throughout this paper, some results of the general non-monotone AS can be found in [12]. Compartmented AS was introduced by Simmons [14]. After that, Brickell [2] gave a more general family, that is the so-called *compartmented access structure with lower bounds (LCAS)* in [16]. There is an efficient and probabilistic SSS for the AS [20]. Recently, Farràs et al. [9, 10] characterized some new ideal compartmented ASs, such as the *compartmented access structure with upper and lower bounds* and the *compartmented access structures with hierarchical compartments (CASHC)*. Some SSS for certain compartmented AS can be found in [19]. Following the work of Farràs et al. [9], Wang et al. [18] presented the *compartmented access structures with strictly lower bounds (SLCAS)*. The new AS can provide better fairness among the groups in recovering the secret. However, both Farràs [9] and Wang [18] didn't give efficient, ideal and perfect SSSs for these ASs, as by far there is not an efficient algorithm to obtain a representation of a multipartite matroid from a representation of its associated integer polymatroid.

In this paper, we give a perfect (with probability) and ideal SSS for one of the CASHC which were introduced in [9]. Then, we construct a SSS for the SLCAS which was given in [18]. As far as we know, there does not exist any efficient, ideal and perfect schemes for these ASs. Although our schemes are probabilistic, they are simple and easy understanding for the purpose of practical applications.

## 2 Preliminaries

### 2.1 Secret sharing

In a secret sharing scheme, let $\mathcal{P} = \{p_1, \cdots, p_n\}$ be the set of *participants*. An *access structure* (AS) is a monotone collection $\Gamma \subseteq 2^{\mathcal{P}}$: we have $C \in \Gamma$ if $B \in \Gamma$ and $B \subseteq C$. The notation $2^{\mathcal{P}}$ is the power set of $\mathcal{P}$. Sets in $\Gamma$ are called *authorized* or *qualified*, and sets not in $\Gamma$ are called *unauthorized* or *unqualified*. $B$ is called a minimal qualified set, if $B \in \Gamma$ and for any $C \subsetneq B$ imply that $C \notin \Gamma$. $\Gamma$ can be determined by all the minimal qualified sets [15]. We let $\Delta = 2^{\mathcal{P}} \setminus \Gamma$, $\Delta$ is called an *adversary structure* which is the set of all unauthorized sets. $B \subseteq \mathcal{P}$ is called a maximal unqualified set, if $B$ is an unqualified set and any superset of $B$ is a qualified set. $\Delta$ can be determined by all the maximal unqualified sets [15].

A SSS requires that the participants of qualified set can recover the secret, and the participants from unqualified set cannot get the secret. Furthermore, if participants from unauthorized set cannot get any information of the secret in the information theoretic sense, then such SSS is called *perfect*. A SSS is called *ideal* if $|S_i| = |S|$ for every $1 \le i \le n$, where $S$ is the domain of the secret $s$, and $S_i$ is the share domain of participant $i$. An AS is called ideal if there exists an ideal SSS realizing it. A SSS is called *linear* if the secret $s$ is a linear combination of participants' shares that from qualified set. We define the *probabilistic* secret sharing scheme as in [20]. That is, although $V \in \Gamma$, sometimes the participants in $V$ cannot recover the secret either, but that is only a small probability event.

## 2.2 Compartmented access structure

Every participant in threshold access structure has the same effect when recovering the secret. We can generalize threshold AS like this: we divide $\mathcal{P}$ into several disjoint groups, and every group has its own threshold value. The participants in the same group have the same power just like that in threshold AS. AS like this are called *compartmented* AS.

Farràs et al. [9] found some new ideal compartmented ASs, one of them is the *compartmented access structure with hierarchical compartments (CASHC)*. The definition of the CASHC is given as follows. Through this paper, we use $[m]$ denotes the set $\{1, 2, \cdots, m\}$. For a set $\mathcal{S}$, $b \in_R \mathcal{S}$ denotes that the element $b$ was selected randomly from the set $\mathcal{S}$.

**Definition 1** Let $\mathcal{P} = \bigcup_{i=1}^{m} \mathcal{U}_i$, where $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$, for $i \neq j$. Furthermore, let $\mathcal{U}_i = \bigcup_{j=1}^{n} \mathcal{U}_{ij}$, where $\mathcal{U}_{ik} \cap \mathcal{U}_{il} = \emptyset$, for $k \neq l$. Let $t$ and $b_{i,n} \ge b_{i,n-1} \ge \cdots \ge b_{i,1}$ $(1 \le i \le m)$ be integers such that $\sum_{i=1}^{m} b_{i,n} \ge t + m - 1$. Then the CASHC is

$$\Gamma_1 = \left\{ V \subseteq \mathcal{P} :\ |V| \ge t,\ or\ \exists\, i \in [m],\ \exists\, k \in [n]\ s.t.\ \left| V \cap \bigcup_{j=1}^{k} \mathcal{U}_{ij} \right| \ge b_{i,k} \right\}.$$

In the CASHC, we require the qualified set $V$ at least has cardinality of $t$, or the qualified set must contain $b_{ik}$ participants that come from the first $k$ subgroups in group $\mathcal{U}_i$, for some $i \in [m]$ and $k \in [n]$. The notation $\exists$ in $\Gamma_1$ means that once 1 of $m$ groups and 1 of $n$ subgroups satisfy the condition, then they can recover the secret. For every group $\mathcal{U}_i$, $i \in [m]$, there is a hierarchy among the subgroups $\mathcal{U}_{ij}$, $1 \le j \le n$. When recovering the secret, participants from the subgroup $\mathcal{U}_{il}$ can replace the participants from $\mathcal{U}_{ik}$, for $1 \le l < k \le n$. The hierarchical structure among every group is analogous to the *disjunctive hierarchical AS* in [17]. We will construct a SSS for the CASHC in Section 3.

Wang et al. [18] presented a new ideal compartmented AS, which is called *compartmented access structure with strictly lower bounds (SLCAS)*. We give its definition here.

**Definition 2** Let $\mathcal{P} = \bigcup_{i=1}^{m} \mathcal{U}_i$, where $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$, for $i \neq j$. Let $t,\ t_i,\ (1 \le i \le m),\ k$ be integers satisfy $t \ge \sum_{i=1}^{m} t_i$ and $1 \le k \le \min\{m, t - \sum_{i=1}^{m} t_i\}$. Then the SLCAS is

$$\Gamma_2 = \{V \subseteq \mathcal{P} :\ |V| \ge t,\ |V \cap \mathcal{U}_i| \ge t_i,\ for\ \forall\, i \in [m],\ and\ |\{i :\ |V \cap \mathcal{U}_i| > t_i\}| \ge k\}.$$

If we delete the condition $|\{i : |V \cap \mathcal{U}_i| > t_i\}| \geq k$ in $\Gamma_2$, then the AS becomes the *compartmented access structure with lower bounds (LCAS)* in [9, 16]. AS stated in [18], although LCAS can be used to protect the rights of some 'weak' groups, one or few groups can still dominate the reconstruction. For instance, if $t \gg \sum_{i=1}^{m} t_i$ (the notation $A \gg B$ means that $A$ much larger than $B$) and $|\mathcal{U}_m|$ is large enough, then $t - \sum_{i=1}^{m-1} t_i$ participants in $|\mathcal{U}_m|$ can partaking the recover phase. In this case, $|\mathcal{U}_m|$ performs a more powerful role than the other groups and dominate the reconstructing procedure. But, the SLCAS can provide better fairness among groups, as it requires that at least $k$ groups of participants are strictly greater than the lower bounds $t_i$. We will propose a SSS for the SLCAS in Section 4.

We introduce a lemma, which provides an upper bound for the number of zeros of a multivariate polynomial over a finite field. The lemma is necessary for our proofs in the following sections.

**Lemma 1** *(Schwartz-Zippel Lemma)* [16] *Let $G(z_1, z_2, \cdots, z_k)$ be a nonzero polynomial of $k$ variables over a finite field $\mathbb{F}$ of size $q$. Assume that the highest degree of each of the variables $z_j$ in $G$ is not larger than $d$. Then the number of zeros of $G$ in $\mathbb{F}^k$ is bounded from above by $kdq^{k-1}$.*

## 3 Secret sharing scheme for CASHC

In this section, we design a simple, ideal and perfect (with probability) scheme for $\Gamma_1$. Our method is the bivariate interpolation which was introduced in [16]. Our SSS implementing $\Gamma_1$ is the **Secret Sharing Scheme 1**.

Let $\mathbb{F}_q$ be a finite field and $s \in \mathbb{F}_q$ be the secret to be shared. Set $p_{i,1}(x) = s + a_{i,1}x + \cdots + a_{i,b_{i,1}-1}x^{b_{i,1}-1}$, and $p_{i,j}(x) = p_{i,j-1}(x) + a_{i,b_{i,j-1}}x^{b_{i,j-1}} + \cdots + a_{i,b_{i,j}-1}x^{b_{i,j}-1}$ for $2 \leq j \leq n$, $1 \leq i \leq m$, where $a_{i,k} \in_R \mathbb{F}_q$, $1 \leq k \leq b_{i,n} - 1$.

Let $y_i \in_R \mathbb{F}_q$, $1 \leq i \leq m$, be $m$ distinct elements. Put $L_i(y) = \prod\limits_{1 \leq j \leq m, j \neq i} \frac{y-y_j}{y_i-y_j}$, $1 \leq i \leq m$. We set $p(x, y) = \sum\limits_{i=1}^{m} p_{i,n}(x)L_i(y)$. Let $b_0 = \sum_{i=1}^{m} b_{i,n} - m + 1$ and $\gamma = b_0 - t$. Then our SSS for CASHC is as follows.

### Secret Sharing Scheme 1

(1) For the participant $u_{ijk}$ from $\mathcal{U}_{ij}$, his identity is $x_{ijk} \in_R \mathbb{F}_q$, $x_{ijk} \neq x_{rst}$ for $(i, j, k) \neq (r, s, t)$. The dealer sends $p_{i,j}(x_{ijk})$ to $u_{ijk}$ secretly as his share.

(2) The dealer publishes the values of $p(x, y)$ at $\gamma$ distinct points $(z_i, y'_i) \in_R \mathbb{F}_q^2$, where $y'_i \in \{y_1, y_2, \cdots, y_m\}$, $1 \leq i \leq \gamma$.

We explain the idea of the scheme here. The qualified set $V$ must satisfy $|V \cap \bigcup_{j=1}^{k} \mathcal{U}_{ij}| \geq b_{i,k}$ for some $i \in [m]$, $k \in [n]$, the threshold in this case just like that in Shamir scheme. So we use a polynomial of degree $b_{i,j} - 1$ to distribute the share for participants in $\mathcal{U}_{ij}$, the constant term of the polynomial is the secret. Moreover, the AS requires that participants from $\mathcal{U}_{ij}$ can replace the participants from $\mathcal{U}_{ik}$, $(j < k)$, so we set $p_{i,j}(x)$ as a part of $p_{i,k}(x)$. To ensure that the participant set $V$ with $|V| \geq t$, can recover the secret, we publish $b_0 - t$ values of the $p(x, y)$. The total unknown coefficients in $p(x, y)$ is $b_0$, so $V$ can get the secret by solving a linear equation system. We will analyze the security of the scheme in Theorem 1.

Now, we give an example of this scheme in our real life. Suppose the $n$ participants belong to an organization. The organization have $m$ groups. In every group, some people has more power than others, and there is $n$ levels of power. When a signature requested, $t$ of $n$ participants can make a signature. Moreover, every group that contains certain number of members can represent the organization to make the signature, and members from *superior* level of power can replace the members from *inferior* level to make the signature. Our proposed scheme can be used in this example.

We consider the adversary structure $\Delta_1$ which is the adversary structure of $\Gamma_1$. We have

$$\Delta_1 = \left\{ V \subseteq P : |V| < t, \ and \ \left| V \cap \bigcup_{j=1}^{k} \mathcal{U}_{ij} \right| < b_{ik} \ for \ \forall \, i \in [m], k \in [n] \right\}.$$

**Theorem 1** *If $V \in \Gamma_1$, the participants in $V$ can recover the secret $s$ with probability $1 - C_1/q$, where the constant $C_1$ depends on $b_{i,j}$, $t$ and $m$. If $V \notin \Gamma$, $V$ cannot get any information about the secret with probability $1 - C_2/q$, where the constant $C_2$ depends on $b_{i,j}$, $t$ and $m$.*

*Proof* We prove the first part of the theorem firstly. We just need to consider the minimal qualified set, this is $|V| = t$ or $|V \cap \bigcup_{j=1}^{k} \mathcal{U}_{ij}| = b_{ik}$ for some $i \in [m]$ and $k \in [n]$.

Case 1: $|V| = t$.

In this case, let $|V \cap \mathcal{U}_i| = s_i$, $1 \le i \le m$, obviously, $\sum_{i=1}^{m} s_i = t$. The participants in $V$ can get the linear equation system

$$\mathbf{MX} = \mathbf{F}, \tag{1}$$

where $\mathbf{X} = (s, a_{1,1}, a_{1,2}, \cdots, a_{1,b_{1,n}-1} \cdots, a_{m,1}, \cdots, a_{m,b_{m,n}-1})$, $\mathbf{F}$ is the vector composed of their corresponding shares, and

$$\mathbf{M} = \begin{pmatrix} \mathbf{1}_{s_1} & \mathbf{M}_1 & & & \\ \mathbf{1}_{s_2} & & \mathbf{M}_2 & & \\ \vdots & & \vdots & & \\ \mathbf{1}_{s_m} & & & & \mathbf{M}_m \\ \mathbf{L}_\gamma & H_1 & \mathbf{H}_2 & \cdots & \mathbf{H}_m \end{pmatrix}_{b_0 \times b_0} .$$

The matrices $\mathbf{1}_{s_i}$, $\mathbf{M}_i$ and $\mathbf{H}_i$ are as follows.

$$\mathbf{1}_{s_i} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}_{s_i \times 1}, \ \mathbf{M}_i = \begin{pmatrix} x_{i1} & x_{i1}^2 & \cdots & x_{i1}^{b_{i,n}-1} \\ \vdots & \vdots & & \vdots \\ x_{is_i} & x_{is_i}^2 & \cdots & x_{i,s_i}^{b_{i,n}-1} \end{pmatrix}_{s_i \times (b_{i,n}-1)}, \ 1 \le i \le m.$$

$$\mathbf{L}_\gamma = \begin{pmatrix} \sum_{i=1}^{m} L_i(y_i') \\ \sum_{i=1}^{m} L_i(y_i') \\ \vdots \\ \sum_{i=1}^{m} L_i(y_i') \end{pmatrix}_{\gamma \times 1}, \ \mathbf{H}_i = \begin{pmatrix} L_i(y_i')z_1 & L_i(y_i')z_1^2 & \cdots & L_i(y_i')z_1^{b_{1,n}-1} \\ \vdots & \vdots & & \vdots \\ L_i(y_i')z_\gamma & L_i(y_i')z_\gamma^2 & \cdots & L_i(y_i')z_\gamma^{b_{1,n}-1} \end{pmatrix}_{\gamma \times (b_{i,n}-1)},$$

for $1 \le i \le m$. The equation system has $t + \gamma = b_0$ equations and $b_0$ variables. We only need to prove the event that $|\mathbf{M}| = 0$ happens with a negligible probability, where the notation $|\mathbf{M}|$ denotes the determine of $\mathbf{M}$. We view the determine of $\mathbf{M}$ as a $\gamma$-variate polynomial $g(z_1, z_2, \cdots, z_\gamma)$. There are two cases as follows: the case where $g(z_1, z_2, \cdots, z_\gamma)$

is identically zero and the case that is not. We consider the case $g(z_1, z_2, \cdots, z_\gamma)$ is not identically zero firstly. According to the lemma 1, the number of zero of $g(z_1, z_2, \cdots, z_\gamma)$ in $\mathbb{F}_q^\gamma$ is bounded by $\gamma(b-1)q^{\gamma-1}$, where $b = \max\limits_{1 \le i \le m} b_{i,n}$. Since $z_i$ were randomly selected from $\mathbb{F}_q$, the probability of $(z_1, z_2, \cdots, z_\gamma)$ being one of the zero of $g(z_1, z_2, \cdots, z_\gamma)$ is bounded from above by $\gamma(b-1)/q$. We consider the case $g(z_1, z_2, \cdots, z_\gamma) \equiv 0$. $g(z_1, z_2, \cdots, z_\gamma) \equiv 0$ if and only if all of its coefficients are zero, where each of the coefficients is a polynomial in $b_0$ variables whose degree with respect to each of its variables is bounded by $d = \max\{b-1, m-1\}$. So, the probability of one of the coefficient to be zero is $b_0 d/q$. Then the probability of $g(z_1, z_2, \cdots, z_\gamma) \equiv 0$ is $C/q$, where the constant $C$ depends on $b_{i,n}$, $m$ and $t$.

Case 2: $\exists i \in [m], k \in [n]$ s.t. $\left|V \cap \bigcup_{j=1}^{k} \mathcal{U}_{ij}\right| = b_{i,k}$.

Let $|V \cap \mathcal{U}_{ij}| = \alpha_{ij}$, $\sum_{j=1}^{k} \alpha_{ij} = b_{i,k}$. In this case, $V$ can construct the following equation:

$$\mathbf{MX} = \mathbf{F},$$

where $\mathbf{X} = (s, a_{i,1}, a_{i,2}, \cdots, a_{i,b_{i,k}-1})$, $\mathbf{F}$ is the share vector, and

$$\mathbf{M} = \begin{pmatrix} \mathbf{1}_{\alpha_{i1}} & \mathbf{M}_1 & & \\ \mathbf{1}_{\alpha_{i2}} & & \mathbf{M}_2 & \\ \vdots & & \vdots & \\ \mathbf{1}_{\alpha_{ik}} & & & \mathbf{M}_k \end{pmatrix}_{b_{i,k} \times b_{i,k}} .$$

Here the matrices $\mathbf{1}_{\alpha_{il}}$ and $\mathbf{M}_l$ are as follows:

$$\mathbf{1}_{\alpha_{il}} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}_{\alpha_{il} \times 1}, \quad \mathbf{M}_l = \begin{pmatrix} x_{ij1}^{b_{i,j-1}} & x_{ij1}^{b_{i,j-1}+1} & \cdots & x_{ij1}^{b_{i,j}-1} \\ \vdots & \vdots & & \vdots \\ x_{ij\alpha_{ij}}^{b_{i,j-1}} & x_{ij\alpha_{ij}}^{b_{i,j-1}+1} & \cdots & x_{ij\alpha_{ij}}^{b_{i,j}-1} \end{pmatrix}_{\alpha_{ij} \times (b_{i,j} - b_{i,j-1})},$$

where $b_{i,0} = 1$ and $1 \le l \le k$. Just like the analysis in Case 1, we can get the result that the probability of $|\mathbf{M}| = 0$ is $b_{i,k}(b_{i,k}-1)/q$. Up to now, we have proved that the qualified set $V$ can reconstruct the secret with probability $1 - C_1/q$, where the constant $C_1$ depends on $b_{i,j}$, $t$ and $m$.

Next, we prove the second part of this theorem. Let $V$ be the maximal unqualified set, that is, $|V| = t-1$ and $|V \cap \bigcup_{j=1}^{k} \mathcal{U}_{ij}| = b_{i,k} - 1$ for every $i \in [m]$ and $k \in [n]$. For any $i \in [m]$ and $k \in [n]$, the participants in $V$ only can construct the linear equation system $\mathbf{M}_i\mathbf{X} = \mathbf{F}$, where $\mathbf{X} = (s, a_{i,1}, a_{i,2}, \cdots, a_{i,b_{i,k}-1})$, $\mathbf{F}$ is the vector of shares, and

$$\mathbf{M}_i = \begin{pmatrix} 1 & x_{i1} & x_{i1}^2 & \cdots & x_{i1}^{b_{i,k}-1} \\ & & \vdots & & \\ 1 & x_{ib_{i,k}-1} & x_{ib_{i,k}-1}^2 & \cdots & x_{ib_{i,k}-1}^{b_{i,k}-1} \end{pmatrix}_{(b_{i,k}-1) \times b_{i,k}} .$$

We need to show that the vector $\mathbf{e}_1 = (1, 0, \cdots, 0)$ is most probably not spanned by the rows of $\mathbf{M}_i$. In other words, we need to prove that the vector $\mathbf{e}_1 = (1, 0, \cdots, 0)$ cannot be spanned by the rows of $\mathbf{M}_i$ with probability close to 1, where the probability is calculated over all the possible $\mathbf{M}_i$ in the finite field. Let $\mathbf{M}_i' = \binom{\mathbf{e}_1}{\mathbf{M}_i}$, we claim that the probability of $|\mathbf{M}_i'| = 0$ is $(b_{i,k} - 1)^2/q$. The proof is similar to that in the first part of the theorem. Moreover, if the participants in $V$ use the public $\gamma$ points of $p(x, y)$, they can construct $b_0 - 1$ linear equations with respect to $b_0$ variables. By the same method, we can conclude that $V$ cannot get any information about the secret with probability $1 - C_2/q$, where the constant $C_2$ depends on $b_{i,j}$, $t$ and $m$. □

## 4 Secret sharing schemes for SLCAS

In this section, we consider the SSS for $\Gamma_2$. Our SSS for this AS is the **Secret Sharing Scheme 2**. The SSS can be seen as the generalization of the scheme for LCAS in [20].

### Secret Sharing Scheme 2

(1) Let $s \in \mathbb{F}_q$ be the secret, $x_i \in \mathbb{F}_q$, $1 \le i \le m$, are distinct nonzero element. Let $f(x) = \sum_{i=0}^{k-1} a_i x^i$, $p_i(y) = \sum_{j=0}^{t_i} b_{i,j} y^j$ and $R(z) = \sum_{i=1}^{l} c_i z^i$, where $a_i \in_R \mathbb{F}_q, b_{i,j} \in_R \mathbb{F}_q$ and $c_i \in_R \mathbb{F}_q$ such that $s = a_0 + c_1 + \sum_{i=1}^{m} b_{i,1}$. Moreover, $b_{i,0} = f(x_i)$, $1 \le i \le m$, and $l = t - \sum_{i=1}^{m} t_i - k$. Put $Q_i(y, z) = p_i(y) + R(z)$.

(2) Participant $u_{ij}$ from $\mathcal{U}_{ij}$, uniquely identified by $(x_i, y_{ij}, z_{ij})$, $y_{ij}, z_{ij} \in \mathbb{F}_q$. The dealer sends $Q_i(y_{ij}, z_{ij})$ to $u_{ij}$ as his share.

The adversary structure $\Delta_2$ of $\Gamma_2$ is as follows.

$$\Delta_2 = \{V \subseteq P : |V| \le t - 1,\ or\ \exists i \in [m], s.t.\ |V \cap \mathcal{U}_i| \le t_i - 1,$$
$$or\ \ |\{i : \ |V \cap \mathcal{U}_i| > t_i\}| \le k - 1\}.$$

We discuss the security of the scheme for $\Gamma_2$ in the following Theorem 2.

**Theorem 2** *If $V \in \Gamma_2$, the participants in $V$ can recover the secret with probability $1 - C_3/q$, where the constant $C_3$ depends on $k$, $t$ and $t_i$. If $V \notin \Gamma_2$, $V$ cannot get any information about the secret with probability $1 - C_4/q$, where the constant $C_4$ depends on $t$, $t_i$ and $k$.*

*Proof* Suppose that $V$ is a minimal qualified set, i.e. that is $|V| = t$ and $|V \cap \mathcal{U}_i| = s_i \ge t_i$ for any $i \in [m]$, $\sum_{i=1}^{m} s_i = t$, and $|\{i : |V \cap \mathcal{U}_i| > t_i\}| = k$. The participants in $V$ can construct the linear equation system: $\mathbf{MX} = \mathbf{F}$, where $\mathbf{X} = (a_0, a_1, \cdots, a_{k-1}, b_{1,1}, \cdots, b_{1,t_1}, \cdots, b_{m,1}, \cdots, b_{m,t_m}, c_1, \cdots, c_l)$, $\mathbf{F}$ is the vector of shares, and

$$\mathbf{M} = \begin{pmatrix} \mathbf{W}_1 & M_1 & & & \mathbf{N}_1 \\ \mathbf{W}_2 & & M_2 & & \mathbf{N}_2 \\ & & & \vdots & \\ \mathbf{W}_m & & & M_m & \mathbf{N}_m \end{pmatrix}_{t \times t},$$

with

$$\mathbf{W}_i = \begin{pmatrix} 1 & x_i & \cdots & x_i^{k-1} \\ 1 & x_i & \cdots & x_i^{k-1} \\ & & \vdots & \\ 1 & x_i & \cdots & x_i^{k-1} \end{pmatrix}_{s_i \times k}, \mathbf{M}_i = \begin{pmatrix} y_{i1} & y_{i1}^2 & \cdots & y_{i1}^{t_i} \\ y_{i2} & y_{i2}^2 & \cdots & y_{i2}^{t_i} \\ & & \vdots & \\ y_{is_i} & y_{is_i}^2 & \cdots & y_{is_i}^{t_i} \end{pmatrix}, \mathbf{N}_i = \begin{pmatrix} z_{i1} & z_{i1}^2 & \cdots & z_{i1}^{l} \\ z_{i2} & z_{i2}^2 & \cdots & z_{i2}^{l} \\ & & \vdots & \\ z_{is_i} & z_{is_i}^2 & \cdots & z_{is_i}^{l} \end{pmatrix},$$

for each $1 \leq i \leq m$. By the same method used in Theorem 1, we can prove that the probability of $|\mathbf{M}| = 0$ is $C_3/q$, where $C_3$ depends on $k, t$ and $t_i$. So $V$ can get the secret with probability $1 - C_3/q$.

Now, we prove the second part of the theorem. Assuming that $V$ is a maximal unqualified set, let $A \triangleq \{i : |V \cap \mathcal{U}_i| > t_i\}$, then there are three cases:

Case 1: $|V| = t - 1, |V \cap \mathcal{U}_i| \geq t_i, \forall i \in [m]$ and $|A| \geq k$.

The participants in $V$ can construct $t - 1$ equations with respect to $t$ variables. We can conclude that $V$ cannot get any information about the secret with probability $1 - C_4/q$, where the constant $C_4$ depends on $t, t_i, k$. The proof goes along the sam line of arguments as in the proof of Theorem 1.

Case 2: $\exists i \in [m],\ s.t.\ |V \cap \mathcal{U}_i| = t_i - 1$ and $|V \cap \mathcal{U}_j| = |\mathcal{U}_j|$, for $j \neq i$.

In this case, the participants in $V$ cannot recover $b_{i,1}$, as they only can construct the linear equation system $\mathbf{M}_i\mathbf{X} = \mathbf{F}$ that involving $b_{i,1}$, where $\mathbf{X} = (b_{i,1}, b_{i,2}, \cdots, b_{i,t_i})$, $\mathbf{F} = (Q_i(y_{i,1}, z_{i,1}) - R(z_{i,1}) - f(x_i), \cdots, Q_i(y_{i,t_i-1}, z_{i,t_i-1}) - R(z_{i,t_i-1}) - f(x_i))$ and

$$\mathbf{M}_i = \begin{pmatrix} y_{i,1} & y_{i,1}^2 & \cdots & y_{i,1}^{t_i} \\ y_{i,2} & y_{i,2}^2 & \cdots & y_{i,2}^{t_i} \\ & & \vdots & \\ y_{i,t_i-1} & y_{i,t_i-1}^2 & \cdots & y_{i,t_i-1}^{t_i} \end{pmatrix}_{t_i-1\times t_i} .$$

Participants from $V \cap \mathcal{U}_j$ with $j \neq i$, have no contributions to the recovery of the $b_{i,1}$. So $V$ cannot get any information about the secret from the security of Shamir scheme.

Case 3: $|A| = k - 1, |V \cap \mathcal{U}_j| = t_j$ for $j \notin A$, and $|V \cap \mathcal{U}_j| = |\mathcal{U}_j|$ for $j \in A$.

The participants of $V$ can reconstruct $b_{i,0}$ only when $|V \cap \mathcal{U}_i| > t_i$. Since $b_{i,0} = f(x_i)$ and $deg(f) = k - 1$, the participants can recover $a_0$ only when they have $k$ distinct values $f(x_i)$. That is to say, they can recover $a_0$ only when $|A| \geq k$. So $V$ cannot get any information about the secret in this case. □

Next, we give an example of $\Gamma_2$ and use our **Secret Sharing Scheme 2** to realize it.

*Example 1* Let $\mathcal{P} = \bigcup_{i=1}^{3} \mathcal{U}_i, \mathcal{U}_i \cap \mathcal{U}_j = \emptyset$ for $i \neq j$. Suppose that $m = 3, t_1 = 2, t_2 = 3, t_3 = 3, t = 12,$and $k = 2$. We have the access structure $\Gamma = \{V \subseteq \mathcal{P} : |V| \geq 12,\ |V \cap \mathcal{U}_i| \geq t_i,\ for\ \forall i \in [3],\ |\{i : |V \cap \mathcal{U}_i| > t_i\}| \geq 2\}$. Let $s \in \mathbb{F}_q$ be the secret, we design SSS for the $\Gamma$ as follows:

Let $f(x) = a_0 + a_1x$, $p_1(y) = b_{1,0} + b_{1,1}y + b_{1,2}y^2$, $p_2(y) = b_{2,0} + b_{2,1}y + b_{2,2}y^2 + b_{2,3}y^3$, $p_3(y) = b_{3,0} + b_{3,1}y + b_{3,2}y^2 + b_{3,3}y^3$, $R(z) = c_1z + c_2z^2$. The coefficients $a_0, a_1, c_1, c_2, b_{i,j},\ 1 \leq i \leq 3,\ 1 \leq j \leq t_i$, were selected randomly from $\mathbb{F}_q$ such that $s = c_1 + a_0 + b_{1,1} + b_{2,1} + b_{3,1}$. Moreover, $b_{i,0} = f(x_i)$, $1 \leq i \leq 3$, where $x_i \in_R \mathbb{F}_q$. Put $Q_i(y, z) = p_i(y) + R(z)$, $1 \leq i \leq 3$.

The participant $u_{i,j}$ in $\mathcal{U}_i$ is uniquely identified by $(x_i, y_{i,j}, z_{i,j})$, where $y_{i,j}, z_{i,j} \in_R \mathbb{F}_q$. The dealer send $Q_i(y_{i,j}, z_{i,j})$ to $u_{i,j}$ as his share. We discuss the security of the above scheme in the following cases.

Let $V \subseteq \mathcal{P}$, $V = 12$, $|V \cap \mathcal{U}_1| = 2$, $|V \cap \mathcal{U}_2| = 5$ and $|V \cap \mathcal{U}_3| = 5$. $V$ is a minimal qualified set. The participants in $V$ can construct the equation

$\mathbf{MX} = \mathbf{F}$, where $\mathbf{X} = (a_0, a_1, b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2}, b_{2,3}, b_{3,1}, b_{3,2}, b_{3,3}, c_1, c_2)$, $\mathbf{F} = (Q_1(y_{1,1}, z_{1,1}), Q_1(y_{1,2}, z_{1,2}), Q_2(y_{2,1}, z_{2,1}), \cdots, Q_2(y_{2,5}, z_{2,5}), Q_3(y_{3,1}, z_{3,1}), \cdots, Q_3(y_{3,5}, z_{3,5}))$, and

$$\mathbf{M} = \left(\begin{array}{cccccccccccc}
1 & x_1 & y_{1,1} & y_{1,1}^2 & & & & & & & z_{1,1} & z_{1,1}^2 \\
1 & x_1 & y_{1,2} & y_{1,2}^2 & & & & & & & z_{1,2} & z_{1,2}^2 \\
1 & x_2 & & & y_{2,1} & y_{2,1}^2 & y_{2,1}^3 & & & & z_{2,1} & z_{2,1}^2 \\
1 & x_2 & & & y_{2,2} & y_{2,2}^2 & y_{2,2}^3 & & & & z_{2,2} & z_{2,2}^2 \\
\vdots & & & \vdots & & \vdots & & & & & \vdots & \\
1 & x_2 & & & y_{2,5} & y_{2,5}^2 & y_{2,5}^3 & & & & z_{2,5} & z_{2,5}^2 \\
1 & x_3 & & & & & & y_{3,1} & y_{3,1}^2 & y_{3,1}^3 & z_{3,1} & z_{3,1}^2 \\
1 & x_3 & & & & & & y_{3,2} & y_{3,2}^2 & y_{3,2}^3 & z_{3,2} & z_{3,2}^2 \\
\vdots & & & \vdots & & \vdots & & & & & \vdots & \\
1 & x_3 & & & & & & y_{3,5} & y_{3,5}^2 & y_{3,5}^3 & z_{3,5} & z_{3,5}^2
\end{array}\right)_{12\times 12}$$

So the probability of $\mathbf{M} = 0$ is about $81/q$, the participants in $V$ can get the secret $s$ with probability $1 - 81/q$. When $q > 8.1 \times 10^3$, the probability of $V$ can recover $s$ is larger than 0.99.

Let $V \subseteq \mathcal{P}$, $|V| = 11$, $|V \cap \mathcal{U}_1| = 2$, $|V \cap \mathcal{U}_2| = 5$ and $|V \cap \mathcal{U}_3| = 4$. $V$ is a maximal unqualified set. In this case, $V$ can construct $\mathbf{M'X} = \mathbf{F}'$, where $\mathbf{X}$ is the vector as above, $\mathbf{F}'$ is composed of the first 11 elements of the vector $\mathbf{F}$ and $\mathbf{M}'$ is composed of the first 11 rows of $\mathbf{M}$. Let $\mathbf{e}_1 = (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$, we need to prove that $\mathbf{e}_1$, most probability, cannot be span by the rows of $\mathbf{M}'$. After analysis, we get that the probability of $\begin{vmatrix} \mathbf{e}_1 \\ \mathbf{M}' \end{vmatrix} = 0$ is about $75/q$. So $V$ cannot get any information about the secret with probability $1 - 75/q$ approximately. Put $V \subseteq \mathcal{P}$: $|V| = n - |\mathcal{U}_1| + 1$, $|V \cap \mathcal{U}_1| = 1$, $|V \cap \mathcal{U}_2| = \mathcal{U}_2$ and $|V \cap \mathcal{U}_3| = \mathcal{U}_3$. $V$ is a maximal unqualified set. In this case, there are only one linear equation that related to the variable $b_{1,1}$:

$$\left(y_{1,1}, y_{1,1}^2\right)\begin{pmatrix} b_{1,1} \\ b_{1,2} \end{pmatrix} = Q(y_{1,1}, z_{1,1}) - R(z_{1,1}) - f(x_1).$$

But the equation has two variables $b_{1,1}$, $b_{1,2}$. So the participants cannot get any information about $b_{1,1}$. Then $V$ cannot recover the secret.

Let $V \subseteq \mathcal{P}$ : $|V \cap \mathcal{U}_1| = \mathcal{U}_1 + 6$, $|V \cap \mathcal{U}_2| = 3$ and $|V \cap \mathcal{U}_3| = 3$. $V$ is a maximal unqualified set. In this case, participants from $V \cap \mathcal{U}_1$ can recover $b_{1,0} = f(x_1)$, while participants of $V \cap \mathcal{U}_2$ have $\mathbf{M}_2\mathbf{X} = \mathbf{F}$, where $\mathbf{X} = (a_0, a_1, b_{2,1}, b_{2,2}, b_{2,3})$, $\mathbf{F} = \big(Q_2(y_{2,1}, z_{2,1}) - R(z_{2,1}), Q_2(y_{2,2}, z_{2,2}) - R(z_{2,2}), Q_2(y_{2,3}, z_{2,3}) - R(z_{2,3})\big)$ and

$$M_2 = \begin{pmatrix} 1 & x_2 & y_{2,1} & y_{2,1}^2, y_{2,1}^3 \\ 1 & x_2 & y_{2,2} & y_{2,2}^2, y_{2,2}^3 \\ 1 & x_2 & y_{2,3} & y_{2,3}^2, y_{2,3}^3 \end{pmatrix}.$$

The linear equation system has only three equations with four variables. So they cannot recover $b_{2,0} = f(x_2) = a_0 + a_1 x_2$. Similarly, participants of $V \cap \mathcal{U}_3$ cannot get $b_{3,0} = f(x_3)$. Up to now, $V$ only get the value of $f(x_1)$. Hence $V$ cannot recover $a_0$, and $V$ can not reconstruct the secret further.

## 5 Conclusions

We devised ideal secret sharing scheme for CASHC and SLCAS respectively. Our ideas come from the bivariate interpolation [16]. Since these ASs are generations of some known ASs, our proposed schemes may be suitable for much real-world scenarios. Although our schemes have a probability of failure, but as we know the probability is negligible when the cardinality of the finite field is big enough. Obviously, the complexity of the computation of the SSS increase with the increase of the cardinality of the field. In the process of distribution, we only need the operations of addition and multiplication. The share distribution process is analogous to that of Shamir scheme. In the process of recovery, we need to solve a system of linear equations. By using the Gauss elimination which needs $O(n^3)$ operations over the field, we can finish the reconstruction of the secret. In order to implement the proposed scheme more easier, we can construct the tables of addition and multiplication operation over the finite field. The processes of distribution and reconstruction can be speeded up by finding these tables.

We should note that the open problem in [9, 18] that finding ideal, perfect and efficient SSS for these ASs are not solved here. So far there are not any ideal, efficient and perfect (without the probability) schemes for these ASs. The skill in [17] may have some inspiration for us. If we can allocate the identity of participant reasonably, we may get the deterministic scheme for these ASs without the probability.

**Acknowledgments** The authors are very grateful to the reviewers and the Editor, for their comments and suggestions that improved the presentation and quality of this paper. This research was supported by NTU Tier 1 grant RG143/14, the National Key Basic Research Program of China (Grant No. 2013CB834204), and the National Natural Science Foundation of China (Grant Nos. 61571243 and 61171082).

## References

1. Blakley, G.R.: Safeguarding cryptographic keys, National Computer Conference, New York, Montvale, NJ, USA, vol. 48 of AFIPS Conference Proceedings (1979)
2. Brickell, E.F.: Some ideal secret sharing schemes. J. Combin. Math. Combin. Comput. **9**(2), 105–113 (1989)
3. Beimel, A.: Secret-Sharing schemes: A survey. Proc. IWCC 2011, Qingdao, China LNCS **6639**, 11–46 (2011)
4. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. Proc. Adv. Cryptol, LNCS **403**, 27–35 (1990)
5. Ding, C., Laihonen, T., Renvall, A.: Linear multi-secret sharing schemes and error-correcting codes. J. Univ. Comput. Sci. **3**(9), 1023–1036 (1997)
6. Ding, C., Kohel, D., Ling, S.: Secret sharing with a class of ternary codes. Theor. Comput. Sci. **246**, 285–298 (2000)
7. Ding, C., Yuan, J.: Covering and secret sharing with linear codes. In: Discrete Mathematics and Theoretical Computer Science, Lecture Notes in Computer Science 2731, 2003, pp. 11–25. Springer Verlag (2003)
8. Ding, C., Salomaa, A.: Secret sharing schemes with nice access structures. Fundam. Inf. - icae **71**(1-2), 65–79 (2006)
9. Farràs, O., Padró, C., Xing, C., Yang, A.: Natural generalizations of threshold secret sharing. IEEE Trans. Inf. Theory **60**(3), 1652–1664 (2014)
10. Farràs, O., Martí-Farré, J., Padró, C.: Ideal multipartite secret sharing schemes. J. Cryptol. **25**(3), 434–463 (2012)
11. Ito, M., Saito, A., Nishizeki, T.: Multiple assignment scheme for sharing secret. J. Cryptol. **6**(1), 15–20 (1993)
12. Liu, J., Mesnager, S., Chen, L.: Secret Sharing Schemes with General Access Structures. http://eprint.iacr.org/2015/1139.pdf

13. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
14. Simmons, G.J.: How to (really) share a secret. Proc. Adv. Cryptol, LNCS **403**, 390–448 (1990)
15. Stinson, D.R.: An explication of secret sharing schemes. Des. Codes Cryptogr. **2**(4), 357–390 (1992)
16. Tassa, T., Dyn, N.: Multipartite secret sharing by bivariate interpolation. J. Cryptol. **22**(2), 227–258 (2009)
17. Tassa, T.: Hierarchical threshold secret sharing. J. Cryptol. **20**(2), 237–264 (2007)
18. Wang, Y., Wu, Q., W, D., et al.: Further ideal multipartite access structures from integer polymatroids. Sci. China Inf. Sci. **58**(7), 1–13 (2015)
19. Wang, X., Fu, F.-W., Guang, X.: Probabilistic secret sharing schemes for multipartite access structures. IEICE Trans. Fundam. **E99-A**(4), 856–862 (2016)
20. Yu, Y., Wang, M.: A probabilistic secret sharing scheme for a compartmented access structure. Proc. ICICS' 2011, Beijing, China LNCS **7043**, 136–142 (2011)