An Ideal Compartmented Secret Sharing Scheme Based on Linear Homogeneous Recurrence Relations

Jiangtao Yuan[a], Guoai Xu[a,*], Guosheng Xu[a]

[a]*Beijing University of Posts and Telecommunications, Beijing 100876, China, Beijing 100876, China*

Abstract

Multipartite secret sharing schemes are those that have multipartite access structures. The set of the participants in those schemes is divided into several parts, and all the participants in the same part play the equivalent role. One type of such access structure is the compartmented access structure. We propose an ideal and efficient compartmented multi-secret sharing scheme based on the linear homogeneous recurrence (LHR) relations. In the construction phase, the shared secrets are hidden in some terms of the linear homogeneous recurrence sequence. In the recovery phase, the shared secrets are obtained by solving those terms in which the shared secrets are hidden. When the global threshold is t, our scheme can reduce the computational complexity from $O(n^{t-1})$ to $O(n^{\max(t_i-1)}\log n)$, where $t_i < t$. The security of the proposed scheme is based on Shamir's threshold scheme. Moreover, it is efficient to share the multi-secret and to change the shared secrets in the proposed scheme. That is, the proposed scheme can improve the performances of the key management and the distributed system.

Keywords: `secret sharing`, linear homogeneous recurrence relations, compartmented access structure, multi-secret

1. Introduction

Shamir [1] and Blakley [2] proposed the threshold secret sharing schemes in 1979. Their schemes were based on the Lagrange interpolation algorithm and the linear projective geometry, respectively. In the (*t, n*) threshold secret sharing scheme, the secrets

*Corresponding author
Email address: `jiangt_yuan@163.com, xga@bupt.edu.cn` (Guoai Xu)

can be shared among n participants, and t or more users can recover the shared secrets by pooling their shares, since greater than or equal to t participants (Let $P = \{P_1, P_2, ..., P_n\}$ be the set of the participants, where P_i is the i-th participant in the set P, $1 \leq i \leq n$) can construct a qualified subset. Less than t participants cannot get the shared secrets, since less than t participants cannot construct a qualified subset. If the participants of any unqualified subset cannot obtain any information about the shared secrets, then the scheme is called as the *perfect scheme*. The threshold secret sharing schemes proposed by Shamir and Blakley are only special cases when all the participants have the same authority. Many applications were developed based on the secret sharing scheme [3-4]. This is the reason that the secret sharing scheme is still popular today.

The threshold secret sharing schemes have many limitations in some condition. Hence, other access structures were proposed successively. Shamir proposed the weighted threshold secret sharing scheme [1]. The construction of this scheme is simple: take a threshold scheme and give as many shares as its weight to each participant. Nevertheless, the obtained scheme is not ideal anymore. In 1987, Ito et al. first proposed a scheme to achieve the secret sharing on the general access structure [5]. Simmons first proposed the multipartite access structure [7]. Brickell proposed a method to construct an ideal secret sharing scheme for the multilevel and compartmented access structures [6], but it is not efficient. Computational complexity and storage space size are usually used to measure the efficiency of a scheme. The information rate is usually used to measure the efficiency of a secret sharing scheme. Therefore, to improve the efficiency of the secret sharing scheme, many researchers focused on the study of specific families of access structures, such as graph-based access structures [9], weighted threshold access structures [10], bipartite access structures [11]-[13], tripartite access structures [14]-[15], threshold access structures [16]. Especially Farràs et al. gave a complete characterization of the ideal multipartite access structures [17]. The multipartite secret sharing scheme can be divided into two types. The one is the compartmented secret sharing scheme, and the other is the hierarchical secret sharing scheme.

Recently, there were some researches on the compartmented access structure [18-20]. Tassa et al. proposed two types of the compartmented secret sharing schemes

based on the bivariate Lagrange interpolation [8]. Though some of the existing schemes are proved to be ideal and perfect, the above-mentioned methods are not efficient. Farràs et al. used the matroids and the integer polymatroids to study the compartmented access structure [17], [20], and it is easy to determine whether the secret sharing schemes are ideal or not by the matroids and the integer polymatroids. The problem that how to design a scheme to realize a compartmented access structure can be considered as the problem that how to find a representation of a matroid from the presentation of its associated polymatroid [26]. Chen et al. [26] proposed a compartmented secret sharing scheme based on the general polymatroid and the Gabidulin codes, but the scheme is also to try to obtain nonsingular matrices. Later, Chen et al. [27] gave another method based on the idea of [6], this scheme also needed to check many matric for non-singularity. But Farràs et al. [17], [20] showed that it remains open whether or not there exist efficient algorithms to obtain the representations of multipartite matroids from representations of their associated polymatroids in general. Especially, the compartmented access structure is useful in some applications. For example, although the general managers manage all the departments, they can't make decisions about anything. In the production process of a company's products, whether the product is qualified or not, it must be approved by the department leader who manages only the department at which he/she works. Especially, the general managers are not good at a certain technology, but the department leader is good at the technology. That is to say, the completion of the product requires the cooperation of all departments, and a minimum number of employees in each department needs to involve in it. Mashhadi and Dehkordi first introduced the Linear Homogeneous Recurrence (LHR) relations to the (t,n) threshold secret sharing scheme [25]. Later, they introduced the linear non-homogeneous recurrence (LNHR) relations to the secret sharing scheme [21]. But the participants have the equal authority and the qualified subset A satisfies $|A| \geq t$ in Mashhadi and Dehkordis schemes.

The motivation of our scheme is to design an ideal and efficient secret sharing scheme with the access structures which are more general than the threshold access structures. One of the key contributions is to introduce the LHR relations into the multipartite access structure, especially into the compartmented access structure, which

divides the degree t of a polynomial into the low degrees of some polynomials and each low degree equal to a fixed compartment threshold. In the proposed scheme, the compartmented access structure is realized by using the linear homogeneous recurrence (LHR) relations. The LHR relations are suitable for the compartmented access structure since it has the ability to associate each compartment with a different polynomial. It is easy to share multi-secret in our scheme. Each participant holds a share that is as long as the secret. The security of the proposed scheme is based on Shamir's threshold scheme.

The remainder of this paper is organized as follows. Section 2 introduces the basic knowledge of the linear homogeneous recurrence relations and secret sharing scheme. Section 3 gives the proposed scheme. In section 4, we analyze the security of the proposed scheme. Section 5 discusses some important properties of the proposed scheme and its performance. Finally, Section 6 draws our conclusion.

2. Preliminary Knowledge

In this section, first of all, we introduce the basic mathematical knowledge used in the proposed scheme. A detailed description of the linear homogeneous recurrence relations can be found in [21, 22, 23, 28]. We also give a brief description about the perfect scheme, ideal scheme and the compartmented access structure.

2.1. Linear Homogeneous Recurrence Relations

Theorem 1 (Richard [22]) *Let $h_0, h_1, ..., h_j, ...$ be a sequence of integers and Let $\alpha_1, \alpha_2, ..., \alpha_m$ be the distinct roots of the following characteristic equation of the linear homogeneous recurrence relation with constant coefficients:*

$$h_j = a_1 h_{j-1} + a_2 h_{j-2} + \cdots + a_t h_{j-t}, \tag{1}$$

where $a_t \neq 0$, a_i is selected over GF(q) ($j \geq t$) and q is a large prime.

If α_i is a t_i-fold root of the characteristic equation of (1), then the part of the general solution of this recurrence relation corresponding to α_i is given as

$$F_j^{(i)} = c_{i1}\alpha_i^j + c_{i2}j\alpha_i^j + \cdots + c_{it_i}j^{t_i-1}\alpha_i^j$$
$$= (c_{i1} + c_{i2}j + \cdots + c_{it_i}j^{t_i-1})\alpha_i^j$$

Let $f_i(j) = c_{i1} + c_{i2}j + \cdots + c_{it_i}j^{t_i-1}$. *So we can get*

$$F_j^{(i)} = f_i(j)\alpha_i^j.$$

The general solution of the recurrence relation is

$$h_j = F_j^{(1)} + F_j^{(2)} + \cdots + F_j^{(m)},$$

where $t = \sum_{i=1}^{m} t_i$.

If $\alpha_1 = \alpha_2 = \cdots = \alpha_m = \alpha$, then the general solution of the recurrence relation is

$$h_j = F_j, \tag{2}$$

where

$$F_j = (c_1 + c_2 j + \cdots + c_t j^{t-1})\alpha^j.$$

Definition 2 (Richard [22]) *Let* $h_0, h_1, ..., h_j, ...$ *be an infinite sequence of numbers. Its generating function is defined to be the infinite series*

$$g(x) = \sum_{i=0}^{\infty} h_i x^i.$$

The coefficient of x^j *in* $g(x)$ *is the nth term* h_j. *Thus* x^j *acts as a placeholder for* h_j. *A finite sequence* $h_1, ..., h_j$ *can be regarded as the infinite sequence* $h_1, ..., h_j, 0, 0, ...$, *in which all but a finite number of terms equal 0. Hence, every finite sequence has a generating function*

$$g(x) = \sum_{i=0}^{n} h_i x^i,$$

which is a polynomial.

Theorem 2 (Richard [22]) *Suppose that the LHR sequence $\{h_i\}$ is defined as (1), and the characteristic equation $a_1x^{t-1}+\cdots+a_t=x^t$ has m different roots $\alpha_1,\alpha_2,...,\alpha_m$ with multiplicities $t_1,t_2,...,t_m$, where $t_1+t_2+\cdots+t_m=t$. Then the generating function of the sequence $\{h_i\}$ is*

$$g(x)=\frac{R(x)}{(1-a_1x)^{t_1}(1-a_2x)^{t_2}\cdots(1-a_mx)^{t_m}}, \tag{3}$$

where $R(x)$ is a polynomial function of x with the degree at most $t-1$. Thus we can get

$$h_j=f_1(j)\alpha_1^j+f_2(j)\alpha_2^j+\cdots+f_m(j)\alpha_m^j,$$

where $f_i(j)$ is a polynomial function of j with the degree at most t_i-1. Conversely, given such polynomials

$$R(x) \text{ and } (1-a_1x)^{t_1}(1-a_2x)^{t_2}\cdots(1-a_mx)^{t_m},$$

there is a sequence $h_0,h_1,...,h_j,...$ satisfying a linear homogeneous recurrence relation with constant coefficients of order t of the type (1) whose generating function is given by (2).

2.2. Secret Sharing Schemes

In the following section, we will give the definition of the perfect scheme and ideal scheme, and the hierarchical access structure is also listed.

2.2.1. Perfect Scheme and Ideal Scheme

Definition 3 A (*t, n*) threshold secret sharing scheme $\prod: S\times R\longrightarrow S_1\times S_2\times\cdots\times S_n$ over *M*, where *S* is the shared secret space, *R* is a set of random inputs and S_i $(1\le i\le n)$ is the share space, satisfies the following two conditions:

1) For all $A\subseteq M$ and $|A|\ge t$, $H(S|S_A)=0$, where *A* is the subset of the participants, $|A|$ is the number of the participants in the subset *A*, S_A denotes the information of the shares to be obtained by the participants in the subset *A*, and *H* is the entropy.

2) For all $B \subseteq M$ and $|B| < t$, $0 < H(S|S_B) \leq H(S)$. If $H(S|S_B) = H(S)$, then the scheme is called as the *perfect scheme*.

Definition 4 (Tassa [8]) *Let $\sum_{P_i}$ denote the set of possible shares for the participant $M_i \in M$. The information rate of the scheme is defined as*

$$\rho = \min \frac{\log_2 |S|}{\log_2 |\sum_{P_i}|},$$

where $|S|$ denotes the size of the shared secret, and $|\sum_{P_i}|$ denotes the size of the shares saved by the participant M_i. If $\rho = 1$, the scheme is called as the *ideal scheme*.

2.2.2. Compartmented Access Structure

n is used to denote the total number of the participants in the set $P = \{P_1, P_2, ..., P_n\}$, i.e., $n = |P|$. In the compartmented secret sharing scheme, the set P is divided into disjoint compartments $\gamma_1, \gamma_2, ..., \gamma_m$, i.e., $P = \bigcup_{i=1}^{m} \gamma_i$ and $\gamma_i \bigcap \gamma_j = \emptyset, i \neq j$. The participants in the same compartment play an equivalent role. Let t_i be the compartment γ_i threshold. The compartment γ_i contains k_i participants, where $n = \Sigma_{i=1}^{m} k_i$ and $i \in \{1, ..., m\}$. The qualified subset of the compartmented threshold secret sharing scheme contains at least t_i participants from the compartment γ_i, where $i \in \{1, ..., m\}$ and $t_i \leq k_i$. In the proposed scheme, we suppose that the global threshold t is equal to $\sum_{i=1}^{m} t_i$. The compartmented access structure AS is given by

$$AS = \{A \in 2^M | (|A| \geq t) \wedge (\forall j = \{1, ..., m\})(|A \wedge \gamma_j| \geq t_j)\}.$$

3. The Proposed Scheme

Our scheme is based on the linear homogeneous recurrence relations. In the compartmented secret sharing, the set of participants is partitioned into compartments and the shared secrets can be recovered only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold t_i, and the total number of participants is greater than the global threshold t. In our scheme, we suppose that

$t = \sum_{i=1}^{m} t_i$. The proposed scheme consists of three phases, i.e. the initialization phase, the construction phase(share generation phase and share distribution phase) and the recovery phase. The basic idea of the proposed scheme is illustrated as follows. The system is consisted of some participants and a distributor. The distributor generate a LHR relation with m different roots, where m is the number of the disjoint compartment. Then the distributor chooses the shared secrets and hides the shared secrets in some terms of this LHR relation. The difficulty of our scheme is how to generate this LHR relation. The recovery of the shared secrets is realized by solving the general term of the LHR sequence $\{h_i\}$. Then the participants who want to recover the shared secrets get those terms in which the shared secrets are hidden.

3.1. Initialization Phase

In the proposed scheme, suppose that the compartmented access structure is monotone, that is, if there exists A and $A \in AS$ (the access structure), $\forall A' \in 2^M$and $A \subseteq A'$, then we can get $A' \in AS$. Ito et al. presented that if the access structure AS was monotone, then there existed a perfect secret sharing scheme for the access structure [24].

The proposed scheme requires a public bulletin board. Any person has the right to read or download the contents from the public bulletin board. Only the legitimate participants in the system can publish the information to the directory, and modify or update the published content according to their own permissions. The information among the participants are exchanged and distributed on the bulletin board.

The proposed scheme is based on the LHR relation over $GF(q)$, where q is a large prime and $GF(q)$ is the finite field. $s_1, s_2, ..., s_l$ denote l shared secrets that can be shared among the participants. The distributor D selects x_{ij} over $GF(q)$ as the j-th participant's ID in γ_i, where $x_{ij} \in GF(q) \setminus \{1, 2, ..., l\}$ (This makes sure that we can hide the shared secrets in the first terms $h_1, h_2, ..., h_l$ of the sequence) and $i \in \{1, ..., m\}$ and $j \in \{1, ..., k_i\}$. Then the distributor D publishes the ID on the public bulletin board.

3.2. Construction Phase

The dealer D performs the following steps to generate the shares, distribute the shares and hide the shared secrets in the first terms $h_1, h_2, ..., h_l$:

1) The dealer D chooses m different integers $\alpha_1, \alpha_2, ..., \alpha_m$ over $GF(q)$, where each of them is not zero and m corresponds to the number of disjoint compartments of the participants.

2) The dealer D chooses m different polynomials over $GF(q)$. Let $f_1, f_2, ..., f_m$ denote m different polynomials. The degree of the polynomial f_i is equal to $t_i - 1$, and the t_i is the fixed compartment γ_i threshold. That is

$$f_i = f_i(x) = c_{i1} + c_{i2}x + c_{i3}x^2 + \cdots + c_{it_i}x^{t_i-1},$$

where the global threshold t is equal to $\sum_{i=1}^{m} t_i$ and $i \in \{1, 2, ..., m\}$.

3) D computes $f_i(x_{ij})$ and sends the share $f_i(x_{ij})$ to P_{ij} in compartment γ_i privately in a secure channel, where $1 \leq i \leq m$, $1 \leq j \leq k_i$ and P_{ij} denotes j-th participant in compartment γ_i . This participant keeps the share $f_i(x_{ij})$.

4) After all the shares have been sent to the pariticpants through f_i, where $1 \leq i \leq m$. The dealer D computes

$$f_1(j)\alpha_1^j + f_2(j)\alpha_2^j + \cdots + f_m(j)\alpha_m^j \text{ over } GF(q).$$

Let

$$h_j = f_1(j)\alpha_1^j + f_2(j)\alpha_2^j + \cdots + f_m(j)\alpha_m^j \text{ over } GF(q).$$

5) After the general term is obtained, the dealer D continues to compute $h_1, h_2, .., h_l$. Then D hides the shared secrets $s_1, s_2, ..., s_l$ in these terms $h_1, h_2, .., h_l$.

6) The dealer D computes $y_i = h_i - s_i$, where $1 \leq i \leq l$.

7) The dealer D publishes $y_i (1 \leq i \leq l), \alpha_1, \alpha_2, ..., \alpha_m$ and q on the public bulletin board.

Remark 1 From the step 3) above, we know the polynomial f_i corresponds to the compartment γ_i, and just greater or equal to t_i participants in the compartment γ_i can recover the polynomial f_i by pooling the shares.

Remark 2 From Theorem 1, we can determine that h_j is the general solution of a LHR relation with degree t and the roods of the characteristic equation of this LHR relation are $\{\alpha_1, \alpha_2, ..., \alpha_m\}$.

3.3. Recovery Phase

If the participants in the qualified subset want to recover the shared secrets $s_1, s_2, ..., s_l$, they should recover the polynomials $f_1, f_2, ..., f_m$ firstly. From the construction phase, we know the order of the polynomial f_i is $t_i - 1$. t_i is equal to the fixed compartment γ_i threshold and only the participants in the compartment γ_i can recover the polynomial f_i. Since the order of f_i is $t_i - 1$, we need greater or equal to t_i participants in the compartment γ_i to recover the polynomial f_i.

So these participants in the qualified subset contain at least t_i participants from the subset $\gamma_i = \{P_{i1}, P_{i2}, ..., P_{ik_i}\}$ (we use P_{ij} to denote the j-th participant in the compartment γ_i), where $1 \leq i \leq m$ and $1 \leq j \leq k_i$. Suppose that the subset $A \subseteq P$ satisfies these conditions. A participant in the subset A can obtain the share of each participant by the exchange in the secure channel. Assume that the participants in the qualified subset A want to recover the shared secrets. In the subset A, t_i participants from the compartment γ_i pool the shares, where $1 \leq i \leq m$. By using these shares, these participants can determine f_i, where $1 \leq i \leq m$. After all the polynomials $f_1, f_2, ..., f_m$ have been obtained, from Theorem 1 and the public parameters $\alpha_1, \alpha_2, ..., \alpha_m$ on the public bulletin board, the participants in the subset A can determine the general solution of the recurrence relation. That is,

$$h_j = f_1(j)\alpha_1^j + f_2(j)\alpha_2^j + \cdots + f_m(j)\alpha_m^j \pmod{q}. \tag{4}$$

From (4), the participants in the subset A can compute $h_1, h_2, .., h_l$. From the step 6) of the construction phase, the participants in the subset A can obtain the shared secrets by $s_i = h_i - y_i$, where $1 \leq i \leq l$.

3.4. Example

In this subsection, we give a example to show how the dealer D distributes the secrets in the construction phase and the participants recover the shared secrets in the recovery phase.

3.4.1. Initialization phase

1) Suppose that the set P of the participants is divided into two disjoint compartments $\gamma_1 = 4$, $\gamma_2 = 6$, i.e., $|P| = |\gamma_1 \cup \gamma_2| = 10$ and $k_1 = 4, k_2 = 6$. Let $t_1 = 2$ and

$t_2 = 3$.

2) The D randomly selects two shared secrets $s_1 = 5, s_2 = 6$ over $GF(21)$, where the prime $q = 21$. Set $x_{11} = 3, x_{12} = 4, x_{13} = 5, x_{14} = 6, x_{21} = 7, x_{22} = 8, x_{23} = 9, x_{24} = 10, x_{25} = 11, x_{26} = 12$ over $GF(21) \setminus \{0, 1, 2\}$.

3.4.2. Construction phase

1) The D selects two values $\alpha_1 = 2, \alpha_2 = 1$.

2) The D randomly selects two polynomials f_1, f_2 over $GF(21)$. Let $f_1 = 2x + 1 \pmod{21}$ and $f_2 = x^2 + x + 3 \pmod{21}$.

3) The D distributes the share $f_i(x_{ij})$ to the j-th participant P_{ij} in γ_i, where $1 \leq i \leq 2$ and $1 \leq j \leq k_i$. These shares are listed as follows.

$f_1(x_{11}) = 7, f_1(x_{12}) = 9, f_1(x_{13}) = 11, f_1(x_{14}) = 13, f_2(x_{21}) = 17, f_2(x_{22}) = 12, f_2(x_{23}) = 9, f_2(x_{24}) = 8, f_2(x_{25}) = 9, f_2(x_{26}) = 12$.

4) Let $h_j = (2j + 1)2^j + (j^2 + j + 3) \pmod{21}$ and then the D computes $h_1 = 11, h_2 = 8$.

5) D computes $y_1 = 11 - 5 = 6, y_2 = 8 - 6 = 2$.

6) D publishes $\{y_1, y_2\}, \{\alpha_1, \alpha_2\}$ and q.

3.4.3. Recovery phase

Before the participants can recover the shared secrets, these participants should recover the two polynomials f_1, f_2. For $t_1 = 2$ and $t_2 = 3$, a qualified subset must contain at least two participants from γ_1 and three participants from γ_2. These participants recover the shared secrets by exchanging their shares. We suppose two participants P_{11}, P_{13} from γ_1 and three participants P_{21}, P_{23}, P_{24} from γ_2. The two polynomials are recovered as follows.

1) Firstly, we show how the polynomial f_1 is recovered by P_{11}, P_{13}. For the two points (3, 7) and (5, 11), a polynomial can be determined by

$$\begin{aligned} f_1(x) &= 7\frac{x-5}{3-5} + 11\frac{x-3}{5-3} \\ &= 2x + 1 \pmod{21} \end{aligned}$$

2) Secondly, the polynomial f_2 is recovered by P_{21}, P_{23}, P_{24}. For the three points (7, 17), (9, 9) and (10, 8), a polynomial can be determined by

$$\begin{aligned} f_2(x) &= 17\frac{(x-9)(x-10)}{(7-9)(7-10)} + 9\frac{(x-7)(x-10)}{(9-7)(9-10)} + 8\frac{(x-7)(x-9)}{(10-7)(10-9)} \\ &= 17\frac{(x^2-19x+90}{6} - 9\frac{x^2-17x+70}{2} + 8\frac{x^2-16x+63}{3} \pmod{21} \\ &= x^2+x+3 \pmod{21} \end{aligned}$$

3) From the public values $\alpha_1 = 2, \alpha_2 = 1$, these participants can get

$$h_j = (2j+1)2^j + (j^2+j+3) \pmod{21}.$$

4) These participants compute $h_1 = 11, h_2 = 8$.

5) From the public values y_1, y_2, these participants can obtain the two shared secrets through the equation

$$s_i = h_i - y_i, 1 \leq i \leq 2,$$

so $s_1 = 5, s_2 = 6$.

4. Security Analysis

In this section, we will analyse that the unqualified subset cannot obtain the shared secrets and prove that the public values $\alpha_1, \alpha_2, ..., \alpha_m$ cannot leak any information about the shared secrets. First, we give a proposition below.

Proposition 1 If α_i is a t_i-fold root of the characteristic equation of LHR relation and the general solution for this LHR relation is given by

$$h_j = \sum_{i=1}^{m} (\sum_{k=1}^{t_i} c_{ik} j^{k-1}) \alpha_i^j,$$

then its coefficient c_{ik} can be determined by t initial values by solving linear system of equation, where $t = \sum_{i=1}^{m} t_i$.

From (4), we know when the participants in a unqualified subset want to recover the shared secrets, they must recover every polynomial f_i, $1 \leq i \leq m$. Assume that the

number of the participants is $t-1$ in the unqualified subset. If the total number of the participants in the unqualified subset is $t-1$, where $t=\Sigma_{i=1}^{m}t_i$, then there exists the situation that the number of the participants contained in some compartment γ_i is t_i-1.

Theorem 3 *The linear homogeneous recurrence relation is secure for the unqualified participants if and only if the polynomial is secure for the unqualified participants.*

Proof First , we give a analysis that the public values $\alpha_1,\alpha_2,...,\alpha_m$ do not leak any information about the shared secrets. From the public values $\alpha_1,\alpha_2,...,\alpha_m$, the characteristic equation of a LHR relation can be determined, according to Theorem 1. If a LHR relation is given, then the characteristic equation of this LHR relation can be determined and the root of the characteristic equation can be found. Thus the public values $\alpha_1,\alpha_2,...,\alpha_m$ do not leak any information except characteristic equation of a LHR relation. From (4), we have

$$\begin{aligned} &h''_j = h_j-(f_1(j)\alpha_1^j+\cdots+f_{i-1}(j)\alpha_{i-1}^j+\\ &f_{i+1}(j)\alpha_{i+1}^j+\cdots+f_m(j)\alpha_m^j)=f_i(j)\alpha_i^j \pmod q \\ &\Rightarrow h''_j/\alpha_i^j=f_i(j) \pmod q. \end{aligned} \tag{5}$$

For the Theorem 1, h''_j is also the general term of a LHR relation with t_i degree, where the order of the polynomial $f_i(\cdot)$ is t_i-1. We have supposed that the unqualified subset contains $t-1$ participants and t_i-1 out of $t-1$ is in γ_i (Let the t_i-1 random terms be $h_{i_1},h_{i_2},...,h_{i_{t_i-1}}$).

($\Rightarrow$) Suppose that the of the linear homogeneous recurrence relation with t_i degree is secure for the unqualified participants. From the above, we know that public value α_i does not leak any information except the characteristic equation. If the polynomial with degree (t_i-1) is not secure for the unqualified participants, that is to say, the t_i-1 points can determine a polynomial with degree (t_i-1). From (5), we also infer that the t_i-1 values can determine the linear homogeneous recurrence relation with degree t_i. This is contradictory to our assumption.

($\Leftarrow$) Suppose that the polynomial with degree (t_i-1) is secure for the unqualified participants. If the linear homogeneous recurrence relation degree t_i is not secure for

the unqualified participants, then $t_i - 1$ random terms $(h_{i_1}, h_{i_2}, ..., h_{i_{t_i-1}})$ can determine the linear homogeneous recurrence sequences. According to (5), so we pick up $t_i - 1$ different terms and then can get $t_i - 1$ different points of the polynomial $f_i(j)$. Since the number of the roots of the $f_i(\cdot)$ is $t_i - 1$ at most in the field $\mathbb{F}$, we can say that $t_i - 1$ points can determine a polynomial wit degree $(t_i - 1)$. This is contradictory to our assumption. ■

Therefore, when the participants in the unqualified subset want to obtain the shared secrets, our scheme is safe. Each share is sent through a secure channel, so we do not discuss about the shares leakage.

5. Discussion

In our scheme, each participant just holds one share to share the secrets $s_i, s_2, ..., s_l$ in the whole recovery process. In this section, we will prove that our scheme is perfect and ideal , and we also prove that it is efficient to distribute multiple secrets.

We first show that the proposed scheme is perfect. So we should prove that for all $A \subseteq P$ and $|A| < t$, $H(S|S_A) = H(S)$. Equivalently, we require that for any shared secrets $s, s' \in S$ and $view_A \in S_A$,

$$\Pr[\prod(s,R)|_A = view_A] = \Pr[\prod(s',R)|_A = view_A],$$

where $view_A$ denotes that the participants in the subset A master the Information of the shares and $A = \{P_1, P_2, ..., P_{t-1}\}$, and s is distributed by the linear homogeneous recurrence (LHR) relation (h_j). we use (h_j) to denote the linear homogeneous recurrence relation. The other s' is distributed through the linear homogeneous recurrence (LHR) relation (h'_j). Since the number of the participants in the subset A is $t - 1$, there exists the situation that the number of the participants contained in some compartment γ_i is less than the threshold t_i. We assume that the participants in the subset A can recover all the polynomials except f_i. Suppose two linear homogeneous recursive (LHR) sequences $\{h_j\}$ and $\{h'_j\}$ satisfy the following conditions. That is

$$h_j = f_1(j)\alpha_1^j + f_2(j)\alpha_2^j + \cdots + f_m(j)\alpha_m^j \pmod q,$$
$$\textit{and}$$
$$h'_j = f'_1(j)\alpha_1^j + f'_2(j)\alpha_2^j + \cdots + f'_m(j)\alpha_m^j \pmod q.$$

The degrees of the polynomials f_i and f'_i are $t_i - 1$. Since we can determine all the polynomials except f_i and f'_i, if we can recover two polynomials f_i and f'_i, then h_j and h'_j can be determined. Thus we can determine the shared secrets s, s'. Since

$$\begin{aligned}
f_i(x_{i2}) &= b_0 + b_1 x_{i2} + \cdots + b_{t_i-1} x_{i2}^{t_i-1} \\
f_i(x_{i3}) &= b_0 + b_1 x_{i3} + \cdots + b_{t_i-1} x_{i3}^{t_i-1} \\
&\vdots \\
f_i(x_{it_i}) &= b_0 + b_1 x_{it_i} + \cdots + b_{t_i-1} x_{it_i}^{t_i-1} \\
&\textit{and} \\
f'_i(x_{i2}) &= b'_0 + b'_1 x_{i2} + \cdots + b'_{t_i-1} x_{i2}^{t_i-1} \\
f'_i(x_{i3}) &= b'_0 + b'_1 x_{i3} + \cdots + b'_{t_i-1} x_{i3}^{t_i-1} \\
&\vdots \\
f'_i(x_{it_i}) &= b'_0 + b'_1 x_{it_i} + \cdots + b'_{t_i-1} x_{it_i}^{t_i-1},
\end{aligned}$$

we can get

$$\begin{aligned}
C(b_0, ..., b_{t_i-1})^T &= (f_i(x_{i2}), \cdots, f_i(x_{it_i}))^T, \\
C(b'_0, ..., b'_{t_i-1})^T &= (f'_i(x_{i2}), \cdots, f'_i(x_{it_i}))^T,
\end{aligned} \tag{6}$$

where

$$C^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ x_{i2} & x_{i3} & \cdots & x_{it_i} \\ \vdots & \vdots & \cdots & \vdots \\ x_{i2}^{t_i-1} & x_{i3}^{t_i-1} & \cdots & x_{it_i}^{t_i-1} \end{bmatrix} \tag{7}$$

and x_{ij} is a participant's ID.

From the characteristic of the Vandermonde matrix, we can deduce $rank(C) = t_i - 1$. There is no unique solution to (6). The probabilities of determining the vector $(b_0, ..., b_{t_i-1})^T$ and the vector $(b'_0, ..., b'_{t_i-1})^T$ are equal. Since in the proposed scheme, when m polynomials are determined, then the shared secrets can be determined. So The probabilities of determining s and s' are equal, i.e.

$$\Pr[\prod(s,R)|_A = view_A] = \Pr[\prod(s',R)|_A = view_A].$$

So $H(S|S_A) = H(S)$. Therefore, the proposed scheme is perfect.

In our scheme, each participant's *ID* is published on the public bulletin board, and each participant's share is selected over $GF(q)$. Each participant just should hold one share, and the shared secrets are selected over $GF(q)$. So the information rate of the proposed scheme reaches the upper bound by one. Therefore, the proposed scheme is ideal.

When the global threshold t is large, it usually takes a lot of computation to obtain the pairs of points of the polynomial. Because the order of the polynomial may also be $t-1$, it costs a lot of time to compute on a polynomial with a large degree. In our scheme, we divide the global threshold t into m small thresholds $t_1, t_2, ..., t_m$, where $t = \sum_{i=1}^{m} t_i$. Each threshold t_i corresponds to a polynomial with the degree $t_i - 1$. Since the global order t is divided into m small low thresholds in the proposed scheme, it is efficient to get the evaluations on these low order polynomials. The computational complexity is reduced from $O(n^{t-1})$ to $O(n^{\max(t_i-1)} \log n)$, where $1 \leq i \leq m$ and $t = \sum_{i=1}^{m} (\deg f_i + 1)$. Therefore, in the construction phase, it is efficient to distribute the shared secrets, and in the recovery phase, it is also efficient to recover the shared secrets.

For safety reasons or a certain requirement, we should change the shared secrets. The process of changing the shared secrets are given as follows.

1) D chooses l new shared secrets.

2) D computes $y_i = h_i - s_i$, where $1 \leq i \leq l$.

3) D updates y_i on the public bulletin board, where $1 \leq i \leq l$.

From the above process, we know the computational cost is low to change the shared secrets.

6. Conclusion

In this paper, based on the linear homogeneous recurrence relations and the compartmented access structure, we propose a compartmented multi-secret sharing scheme. We prove that the proposed scheme is ideal and perfect. The security of our scheme is based on Shamir's threshold scheme. Each polynomial corresponds to a different subset of the participants and the degree of the polynomial is equal to the threshold of the compartment minus one, that is, we divide the t-th degree polynomial into m different polynomials. The sum of the degrees of m different polynomials is equal to $t-m$. It is more efficient to distribute or recover the shared secrets by using some polynomials with low orders than to distribute/recover the shared secrets by using a polynomial with a large order, i.e., the computational complexity is reduced from $O(n^{t-1})$ to $O(n^{\max(t_i-1)}\log n)$. Moreover, our scheme is efficient when we share the multi-secret. Especially, when we want to change the shared secrets, we can find the proposed scheme is more efficient than the existing popular multi-secret sharing schemes that were not based on the linear homogeneous recurrence relations. In the proposed scheme, each participant only needs to hold one share in the whole process.

Acknowledgement

This work was supported by the National Key Research and Development Program of China under Grant 2018YFB0803605 and the National Natural Science Foundation of China under Grant 61897069

References

[1] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in Proc. NCC, AFIPS Press, Montvale, NJ, Vol. 48, pp. 313-317, 1979.

[3] D. Xie, L. Li, H. Peng, et al., "A Secure and Efficient Scalable Secret Image Sharing Scheme with Flexible Shadow Sizes," Plos One, vol. 12, no. 1, 2017.

[4] M. Xiao, J. Wu and S. Zhang, et al., "Secret-sharing-based secure user recruitment protocol for mobile crowdsensing," IEEE INFOCOM, pp. 1-9, 2017.

[5] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," Electronics and Communications, Japan (Part III: Fundamental Electronic Science), vol. 72, no. 9, pp. 56-64, 1989.

[6] E. F. Brickell, "Some ideal secret sharing schemes," Journal of Combinatorial Mathematics & Combinatorial Computing, vol. 434, pp. 468-475, 1989.

[7] G. J. Simmons, "How to (Really) Share a Secret," Conference on the Theory and Application of Cryptography. Springer, New York, NY, pp. 390-448, 1988.

[8] T. Tassa, and N.Dyn, "Multipartite secret sharing by bivariate interpolation," Journal of Cryptology, vol. 22, no. 2 pp. 227-258, 2009.

[9] C. Blundo, A. D. Santis, D. R. Stinson, et al., "Graph decompositions and secret sharing schemes," Journal of Cryptology, vol. 8, no. 1, pp. 39-64, 1995.

[10] A. Beimel, T. Tassa, and E. Weinreb, "Characterizing Ideal Weighted Threshold Secret Sharing," Theory of Cryptography, Springer, Berlin, Heidelberg, 2005.

[11] C. PADRó, and G. SáEZ, "Secret sharing schemes with bipartite access structure," IEEE Transactions on Information Theory, 2000, 46.7: 2596-2604.

[12] S. L. Ng, "A Representation of a Family of Secret Sharing Matroids," Designs Codes & Cryptography, vol. 30, no. 1, pp.5-19, 2003.

[13] S. L. Ng, and M. Walker, "On the Composition of Matroids and Ideal Secret Sharing Schemes," Designs Codes & Cryptography, vol. 24, no.1, pp.49-67, 2001.

[14] Collins, J. Michael, "A Note on Ideal Tripartite Access Structures," IACR Cryptology ePrint Archive, vol. 2002, pp. 193, 2002.

[15] J. Herranz, and G. Saez, "New results on multipartite access structures," Information Security Iee Proceedings, vol. 153, no. 4, pp. 153-160, 2006.

[16] T. Tassa, “Hierarchical Threshold Secret Sharing,” Theory of Cryptography Conference. Springer, Berlin, Heidelberg, pp. 473-490, 2004.

[17] O. Farràs, and J. Martł-Farr et al., “Ideal Multipartite Secret Sharing Schemes,” Journal of cryptology, vol. 25, no. 3, 2012.

[18] A. N. Tentu, and K. Bhavani, A. Basit, et al., “Sequential (t,n) multi secret sharing scheme for level-ordered access structure,” International Journal of Information Technology, vol. 11, pp. 1-11, 2018.

[19] Y. Yu, and M. Wang, “A Probabilistic Secret Sharing Scheme for a Compartmented Access Structure,” International Conference on Information and Communications Security, Springer-Verlag, pp. 136-142, 2011.

[20] O. Farràs, Padró C, C. Xing, et al, “Natural Generalizations of Threshold Secret Sharing,” IEEE Transactions on Information Theory, vol. 60, no. 3, pp. 1652-1664, 2014.

[21] S. Mashhadi, and M. H. Dehkordi, “Two verifiable multi secret sharing schemes based on nonhomogeneous linear recursion and lfsr public-key cryptosystem,” Information Sciences, vol. 294, pp. 31-40, 2015.

[22] B. A. Richard, “Introductory Combinatorics,” fifth ed., China Machine Press, 2009, pp. 216-244.

[23] J. Yuan and L. Li, “A fully dynamic secret sharing scheme,” Information Sciences, vol. 496, 2019.

[24] M. Ito, A. Saito, and T. Nishizeki, “Secret sharing scheme realizing general access structure,” In Proceedings IEEE Globcom, Tokyo, Japan, vol. 87, pp. 99-103, 1987.

[25] M. H. Dehkordi, S. Mashhadi, “New efficient and practical verifiable multi-secret sharing schemes,” Information Sciences, vol. 178, pp. 2262-2274, 2008.

[26] Chen Q, Tang C, Lin Z. Efficient explicit constructions of compartmented secret sharing schemes[J]. Designs, Codes and Cryptography, 2019: 1-28.

[27] Q. Chen, C. Tang et al., Efficient explicit constructions of multipartite secret sharing schemes, ASIACRYPT, vol. 11922, pp. 505-536, 2019.

[28] J. Yuan, J. Yang et al., A New Efficient Hierarchical Multi-secret Sharing Scheme Based on Linear Homogeneous Recurrence Relations, Cryptology ePrint Archive, Report 2020/1612, 2020.