A New Efficient Hierarchical Multi-secret Sharing Scheme Based on Linear Homogeneous Recurrence Relations

Jiangtao Yuan, Jing Yang, Guoai Xu, Xingxing Jia, Fang-Wei Fu and Chenyu Wang

Abstract—Hierarchical secret sharing is an important key management technique since it is specially customized for hierarchical organizations with different departments allocated with different privileges, such as the government agencies or companies. Hierarchical access structures have been widely adopted in secret sharing schemes, where efficiency is the primary consideration for various applications. How to design an efficient hierarchical secret sharing scheme is an important issue. In 2007, a famous hierarchical secret sharing (HSS) scheme was proposed by Tassa based on Birkhoff interpolation, and later, based on the same method, many other HSS schemes were proposed. However, these schemes all depend on Polya's condition, which is a necessary condition not a sufficient condition. It cannot guarantee that Tassa's HSS scheme always exists. Furthermore, this condition needs to check the non-singularity of many matrices. We propose a hierarchical multi-secret sharing scheme based on the linear homogeneous recurrence (LHR) relations and the one-way function. In our scheme, we select m linearly independent homogeneous recurrence relations. The participants in the highly-ranked subsets $\gamma_1, \gamma_2, \cdots, \gamma_{j-1}$ join in the j-th subset to construct the j-th LHR relation. In addition, the proposed hierarchical multi-secret sharing scheme just requires one share for each participant, and keeps the same computational complexity. Compared with the state-of-the-art hierarchical secret sharing schemes, our scheme has high efficiency.

Index Terms—Hierarchical access structure, linear homogeneous recurrence relations, secret sharing scheme, multi-secret sharing scheme

1 Introduction

In a (t, n) threshold secret sharing scheme [1], [21], the secret can be shared among n participants, and any t or more participants can constitute a qualified subset to recover the shared secrets by pooling their shares. All the qualified subsets constitute the access structure of the secret sharing scheme. The secret sharing scheme is *perfect* if the participants of any unqualified subsets cannot obtain any information about the shared secrets. The secret sharing scheme is *ideal* if each share has the same size as the secret.

1.1 Related work

The threshold secret sharing schemes proposed by Shamir [1] and Blakley [21] are two special cases where all the participants have the same privileges. Such threshold secret sharing schemes are restrictive in practice. Hence, in order to improve the practicality of secret sharing, many researchers have focused on specific families of access structures, such as weighted threshold access structure [1], graph-based access structure [5], bipartite access structure [6], and multipartite access structure [4] including compartmented access structure and hierarchical access structure.

In 1979, Shamir [1] proposed the weighted threshold secret sharing scheme. But this scheme is a trivial solution by assigning multiple shares to each participant according to its integral weight, which is inefficient. Then in 1988, Simmons [3] proposed a multipartite access structure and he gave the definition of the compartmented access structure and the hierarchical access structure. After Simmons, Brickell [2] proposed a method to construct an ideal secret sharing scheme for the multilevel and compartmented access structures, but the scheme is not efficient, for the exponential operations required to get nonsingular matrices.

The definition of the multipartite access structure is that all participants in a group are divided into some subsets and the participants in the same subset have the equivalent role. Multipartite access structures are classically formed by the compartmented access structure and the hierarchical access structure. A family of the hierarchical access structure contains the conjunctive hierarchical access structure and the disjunctive hierarchical access structure. An important type of hierarchical access structure is the disjunctive hierarchical access structure with the disjoint levels determined by the strictly monotonic increasing thresholds and this access structure gets much more attention than the conjunctive hierarchical access structure.

The hierarchical threshold access structure is useful for large companies where the staff belong to different levels and have different privileges, for example, managers versus employees. The managers have higher power than the em-

- *Jiangtao Yuan, Guoai Xu and Chenyu Wang are with National Engineering Laboratory of Mobile Network Security, College of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China.*
  E-mail: jiangt_yuan@163.com, xga@bupt.edu.cn
- *Jing Yang and Fang-Wei Fu are with the Chern Institute of Mathematics and LPMC, and Tianjin Key Laboratory of Network and Data Security Technology, Nankai University, Tianjin, 300071, China.*
  E-mail: yangjing0804@mail.nankai.edu.cn, fwfu@nankai.edu.cn
- *Xingxing Jia is with School of Mathematics and Statistics, Lanzhou University, Lanzhou, China.*
  E-mail: jiaxx@lzu.edu.cn
  (First authors: Jiangtao Yuan and Jing Yang; Corresponding authors: Guoai Xu, Xingxing Jia and Fang-Wei Fu)

ployees, and the managers are fewer than the employees. The company requires that five of the staff can recover the secret, but at least two of the five must be managers. If the number of employees is not enough, then the managers are allowed to replace employees. This structure can make the companies have fine management and more efficient. Such hierarchical threshold access structures have attracted many attentions [22], [23]. In those hierarchical threshold secret sharing schemes, the participants are divided into disjoint levels $\gamma_1, \gamma_2, ..., \gamma_m$, where γ_i has higher rank than γ_{i+1}, and the participants in subset γ_i have higher privileges than those in subset γ_{i+1}. And a qualified subset satisfies simultaneously that at least k_1 participants are from the highest level γ_1, and at least $k_2 > k_1$ participants are from $\gamma_1 \cup \gamma_2$ and so on, and $k_m > k_{m-1}$ participants are from $\cup_{i=1}^{m}\gamma_i$.

In 2007, Tassa [8] proposed some hierarchical threshold access structures based on Birkhoff interpolation, and the interpolation matrix must satisfy Polya's condition. However, the Polya's condition is just a necessary condition, furthermore, the sufficient condition is scarcely satisfied. The drawback of the above hierarchical threshold access structure is that the distributor must perform exponential checks when assigning identities and shares to the participants. The problem is that whether there exists an efficient ideal secret sharing scheme for such an access structure.

In 2007, Farràs et al. [7] gave a comprehensive characterization of the ideal multipartite access structures. But they didn't design a secret sharing scheme to realize their multipartite access structures, either. Then these scholars studied the hierarchical secret sharing schemes using the results about integer polymatroids in [9]. These techniques provide a characterization of the hierarchical access structures that admits an ideal and perfect secret sharing scheme [10], [15]. But [9], [10] also didn't give a secret sharing scheme which achieves the multipartite access structures. From their result, we know that finding a solution to construct a multipartite secret sharing scheme can be seen as finding a representation of a matroid from a presentation of its associated polymatroid. However, Farràs et al. [9], [11] said that it is still open whether or not there exist efficient methods to get the representations of multipartite matroids from the representations of their associated polymatroids in general.

Following their ideas, in 2019, Chen et al. [12] gave methods to construct ideal linear schemes realizing the compartmented access structure by the general polymatroid-based method presented in [9] and the Gabidulin codes [14]. Then, Chen et al. [13] used linear algebraic techniques to propose a scheme to realize the multipartite access structure. Based on the integer polymatroids, the main idea of [13] provides a polynomial time algorithm to construct such a matrix M that all the determinants of those special submatrices are nonzero over some finite fields. Even though Chen et al. gave a secret sharing scheme to realize hierarchical access structure, they also need to check the non-singularity of many matrices. So the proposed hierarchical secret sharing schemes were either inefficient or randomized.

In 2008, Dehkordi and Mashhadi [18] firstly introduced the linear homogeneous recurrence (LHR) relations to the (t, n) threshold secret sharing scheme based on the RSA cryptosystem. Later, in [16], they introduced the linear non-homogeneous recurrence relations to the secret sharing scheme based on the linear feedback shift register (LFSR) public-key cryptosystem. But the participants are assumed to have the equal privilege in their schemes [16], [18].

1.2 Our results

The paper is motivated by designing an efficient hierarchical multi-secret sharing scheme by using linear homogeneous tools. We propose a hierarchical secret sharing scheme based on the LHR relations [17] and the one-way function [20].

The main idea of our scheme is listed as follows. The secret distributor randomly selects m different LHR relations. Then, the pseudo shares of the participants from the first level γ_1 are used to construct the first LHR relation, which means that the distributor firstly get this LHR relation and the pseudo shares of the participants are used to initialize this LHR relation. Then the pseudo shares of the participants from the first two levels $\gamma_1 \cup \gamma_2$ are used to construct the second LHR relation and so forth. Then the distributor computes the required terms of these m LHR relations and adds them to get some new values to distribute the shared secrets. If the participants in the qualified subset want to recover the shared secrets, they should solve the general term of m LHR relations at first, and thus they can get the required values, and obtain the shared secrets finally.

The security of the proposed scheme is guaranteed by Shamir's threshold scheme. We require that the participants are semi-honest.

The key contributions of the paper are listed as follows.

1) We introduce the LHR relations into the hierarchical access structure, and avoid many checks of the non-singularity of many matrices in the presented hierarchical secret sharing schemes.

2) Our scheme can share multiple secrets at the same time.

3) Each participant only holds one share during the scheme, and our scheme is both perfect and ideal.

The remainder of this paper is organized as follows. In Section 2, we provide preliminaries of secret sharing scheme and LHR relations. In Section 3, we present a new efficient hierarchical multi-secret sharing scheme. In Section 4, we give the important properties of our scheme. In Section 5, compared with the presented schemes, we prove that our scheme is more efficient with better performance . Finally, we draw the conclusion in Section 6.

2 Preliminaries

2.1 Secret Sharing Schemes

In the following section, firstly, we will give the definition of the secret sharing scheme based on information theory.

Definition 1 Let P denote the set of participants, that is $P = \{P_1, P_2, \cdots, P_n\}$. Then a (t, n) threshold secret sharing scheme $\Pi : S \times R \to S_1 \times S_2 \times \cdots \times S_n$ over P satisfies the following two conditions, where S is the shared secret space, R is a set of random inputs, and S_i $(1 \leq i \leq n)$ is the share space.

1) For all $A \subseteq P$ and $|A| \geq t$, $H(S|S_A) = 0$.

2) For all $B \subseteq P$ and $|B| < t$, $0 < H(S|S_B) \leq H(S)$.

If $H(S|S_B) = H(S)$, then the scheme is referred as the *perfect* secret sharing scheme.

Next, we introduce the hierarchical access structure briefly.

Definition 2 Let $P = \{P_1, P_2, \cdots, P_n\}$ denote the set of the participants and $|P| = n$. In a hierarchical secret sharing scheme, the set P can be divided into disjoint levels $\gamma_1, \gamma_2, \cdots, \gamma_m$, i.e., $P = \cup_{i=1}^{m} \gamma_i$ and $\gamma_i \cap \gamma_j = \emptyset$ for all $1 \leq i < j \leq m$. The level γ_i contains n_i participants for $i \in \{1, 2, \cdots, m\}$, and $\Sigma_{i=1}^{m} n_i = n$. Let $K = \{k_i\}_{i=1}^{m}$ be assorted in ascending order, which means that $0 < k_1 < k_2 < \cdots < k_m \leq n$. Then the $(K, n)-$hierarchical threshold access structure is

$$AS = \{A \subset P : |A \bigcap (\bigcup_{j=1}^{i} \gamma_j)| \geq k_i, \forall i \in \{1, 2, \cdots, m\}\}.$$

2.2 Linear Homogeneous Recurrence Relations

In this section, we give a brief introduction of the linear homogeneous recurrence (LHR) relations. The detailed description of the LHR relations can be found in [17], [19], [24].

Definition 3 A LHR relation $(h_i)_{i \geq 0}$ with the k initial values over a finite field $GF(q)$ where q is a prime is defined by these equations:

$$\begin{cases} h_0 = c_0, h_1 = c_1, \cdots, h_{k-1} = c_{k-1}, \\ h_{i+k} + a_1 h_{i+k-1} + \cdots + a_k h_i = 0 \quad (i \geq 0), \end{cases} \qquad (*)$$

where $c_0, c_1, \cdots, c_{k-1}$ and $a_1, a_2, \cdots, a_k$ are predefined constants over $GF(q)$. k is a positive variable, which is the degree of this LHR relation.

Definition 4 For a LHR relation of $(*)$ with degree k over $GF(q)$, the auxiliary equation of this LHR relation is defined as follows

$$p(x) = x^k + a_1 x^{k-1} + \cdots + a_k = 0.$$

Next we introduce some results used in our scheme.

Theorem 1 Let $(h_i)_{i \geq 0}$ be a LHR relation with degree k over $GF(q)$ and $\alpha_1, \alpha_2, \cdots, \alpha_m$ be distinct roots of its auxiliary equation with multiplicities $k_1, k_2, \cdots, k_m$, respectively. Then the general term for this LHR relation is given by

$$h_i = p_1(i)\alpha_1^i + p_2(i)\alpha_2^i + \cdots + p_m(i)\alpha_m^i, \qquad (*)'$$

where $p_j(i) = c_{j1} + c_{j2} i + \cdots + c_{jk_j} i^{k_j - 1}$ and $\sum_{i=1}^{m} k_i = k$.

And these coefficients c_{jv} $(1 \leq j \leq m, 1 \leq v \leq k_j)$ can be determined by k initial values of the LHR relation of $(*)$.

Proof Let α_j be a k_j-fold root of the auxiliary equation $p(x) = x^k + a_1 x^{k-1} + \cdots + a_k = 0$ of $(*)$ where $1 \leq j \leq m$, then we have:

α_j is a k_j-fold root of $p_0(x) = x^{i-k} p(x)$, i.e., $\alpha_j^i + \Sigma_{v=1}^{k} a_v \alpha_j^{i-v} = 0$;

α_j is a $(k_j - 1)$-fold root of $p_1(x) = x p_0'(x)$, i.e., $i\alpha_j^i + \Sigma_{v=1}^{k} a_v (i - v) \alpha_j^{i-v} = 0$;

α_j is a $(k_j - 2)$-fold root of $p_2(x) = x p_1'(x)$, i.e., $i^2 \alpha_j^i + \Sigma_{v=1}^{k} a_v (i - v)^2 \alpha_j^{i-v} = 0$;

$$\vdots$$

α_j is a 1-fold root of $p_{k_j - 1}(x) = x p_{k_j - 2}'(x)$, i.e., $i^{k_j - 1} \alpha_j^i + \Sigma_{v=1}^{k} a_v (i - v)^{k_j - 1} \alpha_j^{i-v} = 0$.

From the analysis above, we find that $h_i^{(j)} = i^{v-1} \alpha_j^i$ $(1 \leq j \leq m, 1 \leq v \leq k_j)$ satisfies this LHR relation $(h_i)_{i \geq 0}$. Therefore, the linear combination of $h_i^{(j)}$, i.e.,

$$h_i = \sum_{v=1}^{k_1} c_{1v} i^{v-1} \alpha_1^i + \sum_{v=1}^{k_2} c_{2v} i^{v-1} \alpha_2^i + \cdots + \sum_{v=1}^{k_m} c_{mv} i^{v-1} \alpha_m^i$$

$$= p_1(i)\alpha_1^i + p_2(i)\alpha_2^i + \cdots + p_m(i)\alpha_m^i$$

also satisfies this LHR relation $(h_i)_{i \geq 0}$, which means that h_i is the general term of the LHR relation of $(*)$, i.e., the form $(*)'$.

We assume that there is a general term of the LHR relation of $(*)$ satisfying $h_i = H_i$ for $0 \leq i \leq k-1$, where H_i is some predetermined constant over $GF(q)$, i.e., the initial values of this LHR relation. Next, in the equation $(*)'$

$$h_i = \sum_{v=1}^{k_1} c_{1v} i^{v-1} \alpha_1^i + \sum_{v=1}^{k_2} c_{2v} i^{v-1} \alpha_2^i + \cdots + \sum_{v=1}^{k_m} c_{mv} i^{v-1} \alpha_m^i,$$

we substitute h_i with these H_i for $0 \leq i \leq k - 1$. Then, we can obtain a linear system of k equations with k variables c_{jv} where $1 \leq j \leq m$ and $1 \leq v \leq k_j$. If the undetermined coefficient method can be used to determine these c_{jv} uniquely, that is to say, the linear system of equations has the unique solution, then the general term of the LHR relation of $(*)$ has the form $(*)'$.

Next, we only need to prove that the coefficient determinant of this linear system of equations is nonzero.

From the analysis above, we know that the determinant of the coefficient is generalized Vandermonde determinant. For $1 \leq j \leq m$, let

$$D_j = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \alpha_j & \alpha_j & \cdots & \alpha_j \\ \alpha_j^2 & 2\alpha_j^2 & \cdots & 2^{k_j - 1}\alpha_j^2 \\ \vdots & \vdots & & \vdots \\ \alpha_j^{k-1} & (k-1)\alpha_j^{k-1} & \cdots & (k-1)^{k_j - 1}\alpha_j^{k-1} \end{pmatrix}.$$

Then we have the following results, where C is a nonzero constant over $GF(q)$:

$$D = |D_1, D_2, \cdots, D_m| = C \prod_{j=1}^{m} \alpha_j^{\binom{k_j}{2}} \prod_{1 \leq i < j \leq m} (\alpha_j - \alpha_i)^{k_i k_j}.$$

When these $\alpha_1, \alpha_2, \cdots, \alpha_m$ are nonzero and different, the determinant of the coefficient $D \neq 0$, which means that this linear system of equations has a unique solution.

Therefore, these coefficients c_{jv} $(1 \leq j \leq m, 1 \leq v \leq k_j)$ can be determined by k initial values of the LHR relation $(*)$. ■

Corollary 1 If $\alpha_1 = \alpha_2 = \cdots = \alpha_m = \alpha$, then the general term of a LHR relation $(h_i)_{i \geq 0}$ with degree k over $GF(q)$ has the form $h_i = p(i)\alpha^i$, where $p(i) = c_1 + c_2 i + \cdots + c_k i^{k-1}$.

3 The Proposed Scheme

In this section, we present our new hierarchical threshold secret sharing scheme based on the LHR relations. The proposed scheme consists of three phases, namely, initialization phase, construction phase and recovery phase.

3.1 Initialization phase

Let D be the distributor, and $P = \{P_1, P_2, \cdots, P_n\}$ be the set of the participants.

1) D divides the set P into disjoint levels $\gamma_1, \gamma_2, \cdots, \gamma_m$, i.e., $P = \cup_{i=1}^{m} \gamma_i$ and $\gamma_i \cap \gamma_j = \emptyset$ for all $1 \le i < j \le m$. For $1 \le i \le m$, each subset $\cup_{j=1}^{i} \gamma_j$ corresponds to two values $(k_i, \sum_{j=1}^{i} n_j)$, where k_i is the threshold of the subset $\cup_{j=1}^{i}\gamma_j$ and $\sum_{j=1}^{i} n_j$ is the number of participants in subset $\cup_{j=1}^{i}\gamma_j$. Notice that $\Sigma_{i=1}^{m} n_i = n$ and $0 < k_1 < k_2 < \cdots < k_m \le n$.

2) D selects randomly l secrets $key_1, key_2, \cdots, key_l \in GF(q)^*$, where q is a big prime.

3) D selects randomly m different one-way functions $f_1(\cdot)$, $f_2(\cdot)$, $\cdots$, $f_m(\cdot)$ and publishes them.

4) D chooses the share $S_i^j \in GF(q)^*$ with respect to the i-th participant at level γ_j, where $1 \le j \le m$ and $1 \le i \le n_j$.

3.2 Construction phase

Let $N_j = n_1 + n_2 + \cdots + n_j$ denote the number of the participants in $\cup_{i=1}^{j}\gamma_i$. Then the distributor D performs the following steps to distribute the shares:

1) D selects m different integers α_1, α_2, $\cdots$, α_m over $GF(q)^*$ and publishes them.

2) For $1 \le j \le m$, $1 \le i \le N_j$, suppose that the share of the i-th participant at level $\cup_{i=1}^{j}\gamma_i$ is $S_i = S_u^v$, where $1 \le v \le j$, and $1 \le u \le n_v$ and $i = N_{v-1} + u$. In particular, we define $N_0 = 0$ and $N_m = n$.

3) For $1 \le j \le m$ and $1 \le i \le N_j$, D computes the pseudo shares $I_i^j = f_j(S_i) \pmod q$.

4) For $1 \le j \le m$, let $(x - \alpha_j)^{k_j} = x^{k_j} + a_{j1}x^{k_j - 1} + \cdots + a_{jk_j} = 0$ where $a_{ji} \in GF(q)$ and $1 \le i \le k_j$. Then the distributor D constructs the j-th LHR relation $(h_i^{(j)})_{i \ge 0}$ with the k_j initial values, which is defined by

$$\begin{cases} h_0^{(j)} = I_1^j, h_1^{(j)} = I_2^j, \cdots, h_{k_j-1}^{(j)} = I_{k_j}^j, \\ h_{i+k_j}^{(j)} + a_{j1}h_{i+k_j-1}^{(j)} + \cdots + a_{jk_j}h_i^{(j)} = 0, \end{cases} \quad i \ge 0. \tag{1}$$

5) D computes $h_i^{(j)}$ where $1 \le j \le m$ and $k_j \le i \le n + l - 1$.

6) D computes $y_i^j = I_i^j - h_{i-1}^{(j)} \pmod q$ and publishes y_i^j, where $1 \le j \le m$ and $k_j < i \le N_j$.

7) Let $h_i = h_i^{(1)} + h_i^{(2)} + \cdots + h_i^{(m)}$ for $n \le i \le n + l - 1$, then D computes $d_i = key_i - h_{n+i-1} \pmod q$ where $1 \le i \le l$.

8) D publishes $\{d_1, d_2, \cdots, d_l\}$.

The Fig.1 shows how to operate the construction phase, where $\gamma_1 + \gamma_2 + \cdots + \gamma_j$ denotes $\cup_{i=1}^{j}\gamma_i$, $(h_i^{(j)})_{i \ge 0}$ denotes the j-th LHR relation, $\{h_i^{(j)}\}_{i=0}^{n+l-1}$ denotes the term from $h_0^{(j)}$ to $h_{n+l-1}^{(j)}$ of the j-th LHR relations and Pshare denotes the pseudo share.

3.3 Recovery phase

In this section, we present how the shared secrets are recovered.

A subset $A \subset P$ is authorized if and only if it contains at least k_m participants, of whom at least k_{m-1} are from $\cup_{i=1}^{m-1}\gamma_i$, of whom at least k_{m-2} are from $\cup_{i=1}^{m-2}\gamma_i$ and so on. Then we know that A contains at least k_1 participants from γ_1. In the qualified subset, these k_m participants need to recover the general terms of m LHR relations before obtaining the shared secrets. The detailed description is shown as follows.

1) Firstly, k_1 participants in γ_1, i.e., $\{P_i\}_{i \in A^{(1)}}$ $(A^{(1)} \subseteq \{1, 2, \cdots, N_1\})$ can compute their pseudo share by $I_i^1 = f_1(S_i)$.

Next, these participants can compute k_1 terms of the first LHR relation from the following equations:

$$h_{i-1}^{(1)} = \begin{cases} I_i^1, & 1 \le i \le k_1 \\ I_i^1 - y_i^1, & k_1 < i \le N_1 \end{cases}$$

According to Theorem 1, using k_1 points $(i - 1, h_{i-1}^{(1)}/\alpha_1^{i-1})$, these participants can determine the polynomial $p^{(1)}(x)$ with degree $k_1 - 1$ defined as follows.

$$\begin{aligned} p^{(1)}(x) &= \sum_{i \in A^{(1)}} \frac{h_{i-1}^{(1)}}{\alpha_1^{i-1}} \prod_{j \in A^{(1)}}^{j \ne i} \frac{x - (j-1)}{i - 1 - (j-1)} \pmod q \\ &= c_0^{(1)} + c_1^{(1)}x + \cdots + c_{k_1-1}^{(1)}x^{k_1-1} \pmod q. \end{aligned}$$

According to Corollary 1, they can get general term of the first LHR relation $h_i^{(1)} = p^{(1)}(i)\alpha_1^i$.

2) Secondly, k_2 participants in $\gamma_1 \cup \gamma_2$, including at least k_1 participants involving in the recovery of the general term of the first LHR relation from γ_1 and other $k_2 - k_1$ participants from γ_2, i.e., $\{P_i\}_{i \in A^{(2)}}$ $(A^{(2)} = A^{(1)} \cup A_2, A_2 \subseteq \{N_1 + 1, N_1 + 2, \cdots, N_2\})$ can compute their pseudo share by $I_i^2 = f_2(S_i)$.

Next, these participants can compute k_2 terms of the second LHR relation from the following equations:

$$h_{i-1}^{(2)} = \begin{cases} I_i^2, & 1 \le i \le k_2 \\ I_i^2 - y_i^2, & k_2 < i \le N_2 \end{cases}$$

According to Theorem 1, using k_2 points $(i - 1, h_{i-1}^{(2)}/\alpha_2^{i-1})$, these participants can determine the polynomial $p^{(2)}(x)$ with degree $k_2 - 1$ defined as follows:

$$\begin{aligned} p^{(2)}(x) &= \sum_{i \in A^{(2)}} \frac{h_{i-1}^{(2)}}{\alpha_2^{i-1}} \prod_{j \in A^{(2)}}^{j \ne i} \frac{x - (j-1)}{i - 1 - (j-1)} \pmod q \\ &= c_0^{(2)} + c_1^{(2)}x + \cdots + c_{k_2-1}^{(2)}x^{k_2-1} \pmod q. \end{aligned}$$

According to Corollary 1, they can get general term of the second LHR relation $h_i^{(2)} = p^{(2)}(i)\alpha_2^i$.

3) Similarly, corresponding participants repeat the operations above.

Until k_m participants in $P = \cup_{i=1}^{m}\gamma_i$, including at least k_{m-1} participants involving in the recovery of the general term of the $(m-1)$-th LHR relation from $\cup_{i=1}^{m-1}\gamma_i$ and the other $k_m - k_{m-1}$ participants from γ_m, i.e., $\{P_i\}_{i \in A^{(m)}}$ $(A^{(m)} = A^{(m-1)} \cup A_m, A_m \subseteq \{N_{m-1}+1, N_{m-1}+2, \cdots, n\})$ can compute their pseudo share by $I_i^m = f_m(S_i)$.

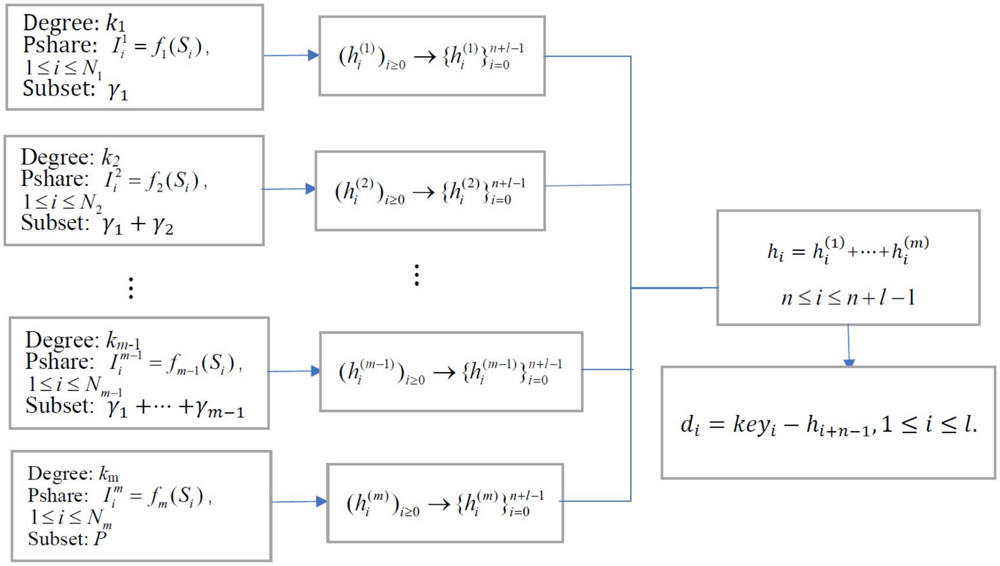
Degree: k_1
Pshare: $I_i^1 = f_1(S_i)$, $1 \le i \le N_1$
Subset: γ_1
$(h_i^{(1)})_{i\ge0} \to \{h_i^{(1)}\}_{i=0}^{n+l-1}$
Degree: k_2
Pshare: $I_i^2 = f_2(S_i)$, $1 \le i \le N_2$
Subset: $\gamma_1 + \gamma_2$
$(h_i^{(2)})_{i\ge0} \to \{h_i^{(2)}\}_{i=0}^{n+l-1}$
⋮
Degree: k_{m-1}
Pshare: $I_i^{m-1} = f_{m-1}(S_i)$, $1 \le i \le N_{m-1}$
Subset: $\gamma_1 + \cdots + \gamma_{m-1}$
$(h_i^{(m-1)})_{i\ge0} \to \{h_i^{(m-1)}\}_{i=0}^{n+l-1}$
Degree: k_m
Pshare: $I_i^m = f_m(S_i)$, $1 \le i \le N_m$
Subset: P
$(h_i^{(m)})_{i\ge0} \to \{h_i^{(m)}\}_{i=0}^{n+l-1}$
$h_i = h_i^{(1)} + \cdots + h_i^{(m)}$
$n \le i \le n+l-1$
$d_i = key_i - h_{i+n-1}, 1 \le i \le l.$

Fig. 1: The construction phase

Next, these participants can compute k_m terms of the m-th LHR relation from the following equations:

$$h_{i-1}^{(m)} = \begin{cases} I_i^m, & 1 \le i \le k_m \\ I_i^m - y_i^m, k_m < i \le n \end{cases}$$

According to Theorem 1, using k_m points $(i-1, h_{i-1}^{(m)}/\alpha_m^{i-1})$, these participants can determine the polynomial $p^{(m)}(x)$ with degree $k_m - 1$ defined as follows:

$$\begin{aligned} p^{(m)}(x) &= \sum_{i\in A^{(m)}} \frac{h_{i-1}^{(m)}}{\alpha_m^{i-1}} \prod_{j\in A^{(m)}}^{j\neq i} \frac{x-(j-1)}{i-1-(j-1)} \pmod q \\ &= c_0^{(m)} + c_1^{(m)} x + \cdots + c_{k_m-1}^{(m)} x^{k_m-1} \pmod q. \end{aligned}$$

According to Corollary 1, they can get general term of the m-th LHR relation $h_i^{(m)} = p^{(m)}(i)\alpha_m^i$.

4) These k_m participants from $P = \cup_{i=1}^m \gamma_i$ add the m general terms of corresponding LHR relations and get $h_i = h_i^{(1)} + h_i^{(2)} + \cdots + h_i^{(m)}$.

5) Finally, these k_m participants can recover the shared secrets by the following equations:

$$key_i = d_i + h_{n+i-1} \pmod q$$

where $1 \le i \le l$.

The Fig.2 shows the main idea of the recovery phase, where Pts denotes the participants, $\gamma_1 + \cdots + \gamma_j$ denotes $\cup_{i=1}^j \gamma_i$, j-LHRR denotes the j-th LHR relation, and $h_i^{(j)}$ denotes the general term of the j-th LHR relation.

Remark 1 For $0 < i < j \le m$, in a hierarchical secret sharing scheme, the participants in γ_i have higher privileges than the participants in γ_j. Therefore, the participants in γ_i can replace the participants in γ_j from the description above. However, these participants must form one of the qualified subset of the hierarchial access structure:

$$AS = \{A \subset P : |A \bigcap (\bigcup_{j=1}^i \gamma_j)| \ge k_i, \forall i \in \{1, 2, \cdots, m\}\}.$$

In particular, at least k_m participants from γ_1 can satisfy the above condition, which means that they can recover the secrets.

3.4 Illustrative Example

In this section, we give an explicit example to demonstrate our scheme and show how the LHR relations are useful in the hierarchical access structure.

Initialization phase

1) Suppose that there are $n = 10$ participants, then the distributor divides them into two level γ_1 and γ_2 satisfying $n_1 = |\gamma_1| = 4$ and $n_2 = |\gamma_2| = 6$. And let the threshold be $k_1 = 2$ and $k_2 = 3$.

2) D selects two secrets $key_1 = 7$ and $key_2 = 9$ from $GF(19)^*$.

3) D selects two one-way functions $f_1(x) = 2^x + 1 \pmod{19}$ and $f_2(x) = 2^{2^x \pmod{19}} + (-1)^x \pmod{19}$.

4) D chooses randomly the share for the participants at the γ_1 be $S_1^1 = 1$, $S_2^1 = 2$, $S_3^1 = 3$, $S_4^1 = 4$ and at the γ_2 be $S_1^2 = 5$, $S_2^2 = 6$, $S_3^2 = 7$, $S_4^2 = 8$, $S_5^2 = 9$, $S_6^2 = 10$.

Construction phase

Let $N_1 = n_1 = 4$ and $N_2 = n_1 + n_2 = 10$, then the distributor D performs the following steps to distribute the shares:

1) D selects two different integers $\alpha_1 = 2$ and $\alpha_2 = 1$ and publishes them.

2) For $j = 1$, $1 \le i \le N_1 = 4$, suppose that the share of the participants at level γ_1 be $S_1 = S_1^1 = 1$, $S_2 = S_2^1 = 2$, $S_3 = S_3^1 = 3$, $S_4 = S_4^1 = 4$.

For $j = 2, 1 \le i \le N_2 = 10$, suppose that the share of the participants at level $\cup_{i=1}^2 \gamma_i$ be $S_1 = S_1^1 = 1$, $S_2 = S_2^1 = 2$, $S_3 = S_3^1 = 3$, $S_4 = S_4^1 = 4$, $S_5 = S_1^2 = 5$, $S_6 = S_2^2 = 6$, $S_7 = S_3^2 = 7$, $S_8 = S_4^2 = 8$, $S_9 = S_5^2 = 9$ and $S_{10} = S_6^2 = 10$.

3) For $j = 1$, D computes the pseudo shares of the participants in γ_1: $I_1^1 = f_1(S_1) = 3$, $I_2^1 = f_1(S_2) = 5$, $I_3^1 = f_1(S_3) = 9$, $I_4^1 = f_1(S_4) = 17$.

For $j = 2$, D computes the pseudo shares of the participants in $\cup_{i=1}^2 \gamma_i$: $I_1^2 = f_2(S_1) = 3$, $I_2^2 = f_2(S_2) = 17$, $I_3^2 = f_2(S_3) = 8$, $I_4^2 = f_2(S_4) = 6$, $I_5^2 = f_2(S_5) = 2$,

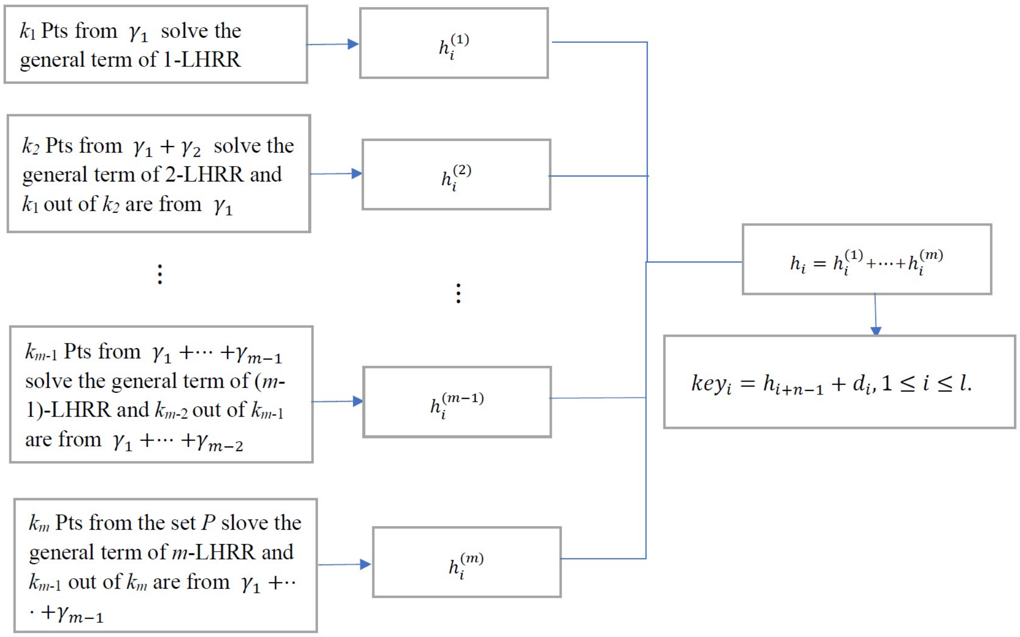
k_1 Pts from γ_1 solve the general term of 1-LHRR
$h_i^{(1)}$
k_2 Pts from $\gamma_1+\gamma_2$ solve the general term of 2-LHRR and k_1 out of k_2 are from γ_1
$h_i^{(2)}$
⋮
⋮
k_{m-1} Pts from $\gamma_1+\cdots+\gamma_{m-1}$ solve the general term of (m-1)-LHRR and k_{m-2} out of k_{m-1} are from $\gamma_1+\cdots+\gamma_{m-2}$
$h_i^{(m-1)}$
k_m Pts from the set P slove the general term of m-LHRR and k_{m-1} out of k_m are from $\gamma_1+\cdots+\gamma_{m-1}$
$h_i^{(m)}$
$h_i = h_i^{(1)}+\cdots+h_i^{(m)}$
$key_i = h_{i+n-1} + d_i, 1 \le i \le l.$

Fig. 2: The recovery phase

$I_6^2 = f_2(S_6) = 15$, $I_7^2 = f_2(S_7) = 5$, $I_8^2 = f_2(S_8) = 0$, $I_9^2 = f_2(S_9) = 0$, $I_{10}^2 = f_2(S_{10}) = 11$.

4) For $j = 1$, let $(x-2)^2 = x^2 - 4x + 4$, and D constructs the first LHR relation $(h_i^{(1)})_{i\geq 0}$ with two initial values, which is defined by

$$\begin{cases} h_0^{(1)} = I_1^1 = 3, h_1^{(1)} = I_2^1 = 5, \\ h_{i+2}^{(1)} - 4h_{i+1}^{(1)} + 4h_i^{(1)} = 0, \end{cases} \quad i \geq 0. \qquad (2)$$

For $j = 2$, let $(x-1)^3 = x^3 - 3x^2 + 3x - 1$, and D constructs the second LHR relation $(h_i^{(2)})_{i\geq 0}$ with three initial values, which is defined by

$$\begin{cases} h_0^{(2)} = I_1^2 = 3, h_1^{(2)} = I_2^2 = 17, h_2^2 = I_3^2 = 8, \\ h_{i+3}^{(2)} - 3h_{i+2}^{(2)} + 3h_{i+1}^{(2)} - h_i^{(2)} = 0, \end{cases} \quad i \geq 0. \quad (3)$$

5) For $j = 1$, using the first LHR relation, D computes $h_2^{(1)} = 8$, $h_3^{(1)} = 12$, $h_4^{(1)} = 16$, $h_5^{(1)} = 16$, $h_6^{(1)} = 0$, $h_7^{(1)} = 12$, $h_8^{(1)} = 10$, $h_9^{(1)} = 11$, $h_{10}^{(1)} = 4$, $h_{11}^{(1)} = 10$.

For $j = 2$, using the second LHR relation, D computes $h_3^{(2)} = 14$, $h_4^{(2)} = 16$, $h_5^{(2)} = 14$, $h_6^{(2)} = 8$, $h_7^{(2)} = 17$, $h_8^{(2)} = 3$, $h_9^{(2)} = 4$, $h_{10}^{(2)} = 1$, $h_{11}^{(2)} = 13$.

6) For $j = 1$, D computes $y_3^1 = 1$, $y_4^1 = 5$ and publishes $\{y_3^1, y_4^1\}$.

For $j = 2$, D computes $y_4^2 = 11$, $y_5^2 = 5$, $y_6^2 = 1$, $y_7^2 = 16$, $y_8^2 = 2$, $y_9^2 = 16$, $y_{10}^2 = 7$ and publishes $\{y_4^2, y_5^2, \cdots, y_{10}^2\}$.

7) D computes $h_{10} = h_{10}^{(1)} + h_{10}^{(2)} = 5$ and $h_{11} = h_{11}^{(1)} + h_{11}^{(2)} = 4$. Then D computes $d_1 = key_1 - h_{10} = 2$ and $d_2 = key_2 - h_{11} = 5$.

8) D publishes $\{d_1, d_2\}$.

Recovery phase

In this phase, for $k_1 = 2$ and $k_2 = 3$, the qualified subset should contain at least two participants from γ_1 and three participants from $\gamma_1 \cup \gamma_2$ simultaneously. Each participant P_i recover the shared secrets by exchanging his/her share S_i with the other participants. Next, we consider how to recover shared secrets under two conditions.

(1) At least two participants in γ_1 and at least one participants in γ_2 can pool their shares to recover the shared secrets by the way mentioned in Section 3.3. We assume that two participants from γ_1 are P_1, P_3 and one participant from γ_2 is P_6.

Firstly, P_1 and P_3 can recover the general term of (2) as follows.

1) P_1 and P_3 can get their pseudo shares $I_1^1 = f_1(S_1) = 3$ and $I_3^1 = f_1(S_3) = 9$.

2) For $1 \leq i \leq 2$, they get $h_0^{(1)} = I_1^1 = 3$. For $2 < i \leq 4$, they get $h_2^{(1)} = I_3^1 - y_3^1 = 8$.

3) According to Theorem 1, using two points $(0, 3/2^0)$ and $(2, 8/2^2)$, the two participants can determine the polynomial $p^1(x)$ with the degree 1:

$$\begin{aligned} p^{(1)}(x) &= \frac{3}{2^0} \cdot \frac{x-2}{0-2} + \frac{8}{2^2} \cdot \frac{x-0}{2-0} \pmod{19} \\ &= 9x + 3 \pmod{19}, \end{aligned}$$

so the general term of (2) is $h_i^{(1)} = (9i+3)2^i$.

Secondly, P_1, P_3 and P_6 can recover the general term of (3) as follows.

4) P_1, P_3 and P_6 can get their pseudo shares $I_1^2 = f_2(S_1) = 3$, $I_3^2 = f_2(S_3) = 8$, and $I_6^2 = f_2(S_6) = 15$.

5) For $1 \leq i \leq 3$, they get $h_0^{(2)} = I_1^2 = 3$ and $h_2^{(2)} = I_3^2 = 8$. For $3 < i \leq 10$, they get $h_5^{(2)} = I_6^2 - y_6^2 = 14$.

6) According to Theorem 1, using three points $(0, 3/1^0)$, $(2, 8/1^2)$ and $(5, 14/1^5)$, the three participants can deter-

mine the polynomial $p^2(x)$ with the degree 2:

$$\begin{aligned} p^{(2)}(x) &= \frac{3}{1^0}\cdot\frac{x-2}{0-2}\cdot\frac{x-5}{0-5} + \frac{8}{1^2}\cdot\frac{x-0}{2-0}\cdot\frac{x-5}{2-5} \\ &+ \frac{14}{1^5}\cdot\frac{x-2}{0-2}\cdot\frac{x-5}{0-5} \pmod{19} \\ &= 17x^2+16x+3 \pmod{19}, \end{aligned}$$

so the general term of (3) is $h_i^{(2)} = 17i^2+16i+3$.

7) Then these participants can get $h_i = h_i^{(1)} + h_i^{(2)} = (9i+3)2^i + (17i^2+16i+3)$.

8) Finally, P_1, P_3 and P_6 can recover the shared secrets by the following equations:

$$key_1 = d_1 + h_{10} = 2+5 = 7,$$

$$key_2 = d_2 + h_{11} = 5+4 = 9.$$

(2) Because the participants in γ_1 have higher privileges than the participants in γ_2 and the participants in γ_1 can replace the participants in γ_2, at least three participants in γ_1 can pool their shares to recover the secrets by the way mentioned in Section 3.3. We assume that three participants from γ_1 are P_1, P_3 and P_4.

Firstly, P_1 and P_3 can recover the general term of (2) using the same way as before, which is $h_i^{(1)} = (9i+3)2^i$.

Secondly, P_1, P_3 and P_4 can recover the general term of (3) as follows.

1) P_1, P_3 and P_4 can get their pseudo shares $I_1^2 = f_2(S_1) = 3$, $I_3^2 = f_2(S_3) = 8$, and $I_4^2 = f_2(S_4) = 6$.

2) For $1 \leq i \leq 3$, they get $h_0^{(2)} = I_1^2 = 3$ and $h_2^{(2)} = I_3^2 = 8$. For $4 < i \leq 10$, they get $h_3^{(2)} = I_4^2 - y_4^2 = 14$.

3)According to Theorem 1, using three points $(0, 3/1^0)$, $(2, 8/1^2)$ and $(3, 14/1^3)$, the three participants can determine the polynomial $p^2(x)$ with the degree 2:

$$\begin{aligned} p^{(2)}(x) &= \frac{3}{1^0}\cdot\frac{x-2}{0-2}\cdot\frac{x-3}{0-3} + \frac{8}{1^2}\cdot\frac{x-0}{2-0}\cdot\frac{x-3}{2-3} \\ &+ \frac{14}{1^3}\cdot\frac{x-0}{3-0}\cdot\frac{x-2}{3-2} \pmod{19} \\ &= 17x^2+16x+3 \pmod{19}, \end{aligned}$$

so the general term of (3) is $h_i^{(2)} = 17i^2+16i+3$.

4) Then, three participants from γ_1 can get $h_i = h_i^{(1)} + h_i^{(2)} = (9i+3)2^i + (17i^2+16i+3)$.

5) Finally, P_1, P_3 and P_4 can recover the shared secrets $key_1 = 7$ and $key_2 = 9$.

4 The Property of Our Scheme

In this section, we will prove that our scheme is secure and show that our scheme is both perfect and ideal.

Firstly, we mainly give an analysis that shows why our scheme keeps secure for the participants in the unqualified subset.

When the participants in an unqualified subset want to recover the shared secrets, they must recover all general terms of m LHR relations at first. For illustration convenience, we suppose that the unqualified subset B satisfies the conditions as follows:

1) $B \bigcap (\bigcup_{i=1}^{j} \gamma_i) = k_j - 1$,

2) $B \bigcap (\bigcup_{i=1}^{t} \gamma_i) \geq k_t$,

where $1 \leq j \leq m$, $1 \leq t \leq m$ and $t \neq j$. That is to say, the unqualified subset can recover all general terms of the $m-1$ LHR relations, except the general term of j-th LHR relation.

Theorem 2 Public values $\alpha_1, \alpha_2, \cdots, \alpha_m$ do not leak any information except the auxiliary equation of the LHR relation.

Proof From the public value α_i, the auxiliary equation $(x-\alpha_i)^{k_i} = 0$ of a LHR relation with degree k_i can be determined. However, without knowing any k_i terms of this LHR relation, the general term of this LHR relation can not be determined. Thus these public values $\alpha_1, \alpha_2, \cdots, \alpha_m$ do not leak any information except the auxiliary equation of the LHR relation. ■

Theorem 3 For $1 \leq j \leq m$,, the LHR relation with degree k_j is secure for the unqualified participants if and only if the polynomial with degree $k_j - 1$ is secure for the unqualified participants.

Proof For $1 \leq j \leq m$, from Corollary 1 and the public value $\alpha_j \neq 0$, we can get

$$h^{(j)}(i) = p^{(j)}(i)\alpha_j^i \Rightarrow p^{(j)}(i) = h^{(j)}(i)/\alpha_j^i \qquad (4)$$

where the degree of $p^{(j)}(i)$ is $k_j - 1$. From Theorem 2, we know that public value α_j does not leak any information except the auxiliary equation of the j-th LHR relation.

($\Rightarrow$) Suppose that the LHR relation with degree k_j is secure for the unqualified participants, which means that $k_j - 1$ values can not determine the general term of a LHR relation with degree k_j. If the polynomial with degree $k_j - 1$ is not secure for the unqualified participants, that is to say, $k_j - 1$ points can determine a polynomial with degree $k_j - 1$. From (4), we also infer that $k_j - 1$ values can determine the general term of a LHR relation with degree k_j, which is contradictory to our assumption.

($\Leftarrow$) Suppose that the polynomial with degree $k_j - 1$ is secure for the unqualified participants. If the LHR relation with degree k_j is not secure for the unqualified participants, then these $k_j - 1$ terms $(h_{i_1}^{(j)}, h_{i_2}^{(j)}, \cdots, h_{i_{k_j-1}}^{(j)})$ can determine the general term of the j-th LHR relation. According to (4), this means that $k_j - 1$ points can determine the polynomial $p^j(i)$ with degree $k_j - 1$, which is contradictory to our assumption. ■

Secondly, we will show that our scheme is both perfect and ideal.

Before we prove this result, we point that each participant only needs to keep one share, but can construct m LHR relations with different pseudo shares. From the description of the recovery phase, we find that those n_1 participants chosen to construct the first LHR relation are used to construct the other $m-1$ LHR relations, too. Because the distributor chooses different one-way functions to compute pseudo shares to construct different LHR relations, all the participants in our scheme only need to keep one share.

For example, in Section 3.4, each participant P_i in γ_1 generates two different pseudo shares $f_1(S_i), f_2(S_i)$ in the construction phase. But each participant P_i in γ_1 just needs to hold one share S_i during the whole scheme.

Theorem 4 Our hierarchical threshold secret sharing scheme is perfect and ideal.

Proof From Theorem 3, we know that the problem whether the participants from the unqualified subset B can recover the general term of the j-th LHR relation can be seen as the problem whether $k_j - 1$ random points can determine the polynomial with degree $k_j - 1$. Obviously, this is impossible because only greater than or equal to k_j points can determine the polynomial with degree $k_j - 1$ uniquely. The probability of determining one shared secret is not greater than that of randomly selecting one shared secret from the predefined finite field $GF(q)$. So our scheme satisfies $H(S|S_B) = H(S)$. Therefore, our scheme is as secure as Shamir's threshold secret sharing scheme, then our scheme is perfect.

Each participant should just hold one share during the whole scheme, and both the share and the shared secrets are selected over $GF(q)$. So the share held by a participant is as long as the shared secret, which means that our scheme is ideal. ■

5 Discussion

In this section, we mainly show some important characteristics of our scheme and compare our scheme with some presented schemes [8], [13].

5.1 Global Threshold

The global threshold of our scheme is k_m, which means that the qualified subsets of our scheme must contain k_m participants. From Theorem 1, we get h_i is a general term of a $(k_1 + k_2 + \cdots + k_m)$-th order LHR relation, however, our scheme only needs k_m participants to recover the shared secrets.

For $j = 1, 2, \cdots, m$, if $k_j - k_{j-1}$ ($k_0 = 0$) participants from the subsets γ_j use their pseudo shares to recover the general term $h_i^{(j)}$, then they must use their other pseudo shares to recover the general terms $h_i^{(j+1)}, \cdots, h_i^{(m)}$. For example, if k_1 participants from γ_1 use their pseudo shares to recover the general term $h_i^{(1)}$, these k_1 participants need to use their other pseudo shares to recover the general terms $h_i^{(2)}$, $h_i^{(3)}$, $\cdots$, $h_i^{(m)}$. Therefore, our scheme needs at least $k_1 + (k_2 - k_1) + \cdots + (k_m - k_{m-1}) = k_m$ participants to recover the shared secrets, which means that the global threshold of our scheme is k_m.

In the illustrative example in Section 3.4, we know that h_i is the general term of a LHR relation with degree 5. However, each participant P_i in γ_1 generates two different pseudo shares $f_1(S_i), f_2(S_i)$ in the recovery phase. For instance, the participants P_1 and P_3 generate $\{f_1(S_1), f_2(S_1)\}$ and $\{f_1(S_3), f_2(S_3)\}$, respectively. Then, $f_1(S_1)$, $f_1(S_3)$ are used to recover the general term of the first LHR relation, and $f_2(S_1)$, $f_2(S_3)$ with $f_2(S_4)$ or $f_2(S_6)$ are used to recover the general term of the second LHR relation. Their different pseudo shares can be used to recover different LHR relations. Therefore, even though the degree of this LHR relation is five, just three participants are required to reconstruct the general terms of two LHR relations. Therefore, the global threshold of this example is $k_2 = 3$.

5.2 Computational complexity

When the threshold of the secret sharing scheme is k_m, the computational complexity of the scheme based on the polynomial usually arrives at $O(n^{k_m - 1})$.

Because the security of our scheme does not depend on the values of $\alpha_1, \alpha_2, \cdots, \alpha_m$, we can let $\alpha_1, \alpha_2, \cdots, \alpha_m$ be special values, such as $1, -1, 2, -2, \cdots$. Therefore the power of α_i is easy to calculate, and the computational complexity of the power of α_i is $O(\log n)$ in our scheme.

So the computational complexity of our scheme is $O(n^{k_m - 1} \log n)$.

5.3 Performance feature

In this section, we give a performance analysis of the schemes in [8], [13], and our scheme.

TABLE 1: Comparing the presented schemes with our scheme

Schemes	Tassa [8]	Chen et al. [13]	Our scheme
The most time cost for calculation	Assigning identities and shares to the participants	Finding nonsingular matrices	Generating or recovering LHR relations
Approach	Birkhoff interpolation	Integer polymatroids and Brickell's method [2]	LHR relations
Time cost	Exponential time	Exponential time	Polynomial time
Multi-secret	NO	NO	YES
Ideal	YES	YES	YES

From the table above, in Tassa's scheme [8], the distributor must perform possibly exponential checks when assigning identities and shares to the participants. Even though Chen et al. [13] gave a hierarchical secret sharing scheme based on the integer polymatroids, the non-singularity of many matrices should be checked, because the main idea of the scheme comes from Brickell [2].

However, in our scheme, the distributor just needs to construct m different LHR relations, compute some required terms and use them to distribute multiple secrets. What's more, the participants only need to do the reconstruction and the summation calculation of the general terms of different LHR relations in our scheme. Although more values need to be published, our scheme avoids many checks. This is because different approaches are used in these schemes. In addition, the time cost of our scheme is polynomial time. Furthermore, our scheme can share multiple secrets at the same time, whereas the other two schemes can only share one secret one time. And our scheme is both perfect and ideal. Therefore, compared with Tassa's and Chen et al.'s scheme, our scheme not only is more efficient, but also has better properties.

6 Conclusion

Based on the LHR relations and the one-way function, we propose a hierarchical multi-secret sharing scheme. We list the characteristics of the proposed scheme as follows.

Our scheme overcomes the drawback that the distributor must perform possibly exponential checks when assigning identities and shares to the participants, when the schemes are based on Birkhoff interpolation. Our scheme also overcomes the drawback of Chen et al.'s scheme in which the non-singularity of many matrices needs to be checked. Our scheme is as secure as Shamir's secret sharing scheme, then our scheme ia also a perfect secret sharing scheme. In addition, each participant just holds only one share during the whole scheme and the share is as long as the secret, which means that our scheme is ideal. Besides, although we need more public values, our scheme can share multiple secrets simultaneously.

In the future, because we assume that the participants are semi-honest in our scheme, we can consider adding verification phase into our scheme without this assumption. What's more, the way used in our scheme can be applied to compartmented secret sharing schemes easily, so we can consider constructing new compartmented secret sharing scheme using LHR relations.

Acknowledgments

This work was supported by the National Key Research and Development Program of China under Grant 2018YFA0704703, 2018YFB0803605, the National Natural Science Foundation of China under Grant 61897069,61971243, the Fundamental Research Funds for the Central Universities of China, and the Nankai Zhide Foundation.

References

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

[2] E. F. Brickell, "Some ideal secret sharing schemes," *J. Combin. Math. & Combin. Comput.*, vol. 9, no. 2, pp. 105-113, 1989.

[3] G. J. Simmons, "How to (really) share a secret," in *Advances in Cryptology-CRYPTO*, Berlin, Germany: Springer-Verlag, 1988, pp. 390-448.

[4] T. Tassa, and N. Dyn, "Multipartite secret sharing by bivariate interpolation," *J. Cryptol.*, vol. 22, no. 2, pp. 227-258, 2009.

[5] C. Blundo, A. Santis, D. R. Stinson, U. Vaccaro, "Graph decompositions and secret sharing schemes," *J. Cryptol.*, vol. 8, no. 1, pp. 39-64, 1995.

[6] C. Padro, and G. Saez, "Secret sharing schemes with bipartite access structure," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2596-2604, 2000.

[7] O. Farràs, J. Martí-Farré, and C. Padró, "Ideal multipartite secret sharing schemes," *Advances in Cryptology-EUROCRYPT*, Berlin, Germany: Springer-Verlag, 2007, pp. 448-465.

[8] T. Tassa, "Hierarchical threshold secret sharing," *J. Cryptol.*, vol. 20, pp. 237-264, 2007.

[9] O. Farràs, J. Martí-Farré, C. Padró, "Ideal multipartite secret sharing schemes," *J. Cryptol.*, vol. 25, no.3, pp. 434-463, 2012.

[10] O. Farràs and C. Padró, "Extending Brickell-Davenport theorem to non-perfect secret sharing schemes," *Des. Codes Cryptograph.*, vol. 74, pp. 495-510, 2015.

[11] O. Farràs, C. Padró, C. Xing, A. Yang, "Natural generalizations of threshold secret sharing," *IEEE Trans. Inf. Theory*, vol. 60, no.3, pp. 1652-1664, 2014.

[12] Q. Chen, C. Tang, Z. Lin, "Efficient explicit constructions of compartmented secret sharing schemes," *Des. Codes Cryptograph.*, vol. 87, pp. 2913-2940, 2019.

[13] Q. Chen, C. Tang, Z. Lin, "Efficient explicit constructions of multipartite secret sharing schemes," in *Advances in Cryptology-ASIACRYPT*, Berlin, Germany: Springer-Verlag, 2019, pp. 505-536.

[14] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Prob. of Inf. Transmiss.*, vol. 21, pp. 1-12, 1985.

[15] O. Farràs and C. Padró, "Ideal hierarchical secret sharing schemes," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3273-3286, 2012.

[16] S. Mashhadi, and M. H. Dehkordi, "Two verifiable multi secret sharing schemes based on nonhomogeneous linear recursion and LRSR public-key cryptosystem," *Inf. Sci.*, vol. 294, pp. 31-40, 2015.

[17] B. A. Richard, *Introductory Combinatorics*, 5th ed. Beijing, China: China Machine Press, pp. 228-258, 2009.

[18] M. H. Dehkordi, S. Mashhadi, "New efficient and practical verifiable multi-secret sharing schemes," *Inf. Sci.*, vol. 178, pp. 2262-2274, 2008.

[19] J. Yuan and L. Li, "A fully dynamic secret sharing scheme," *Inf. Sci.*, vol. 496, pp. 42-52, 2019

[20] O. Goldreich, S. Micali, A. Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority," in *Proc. 19th ACM STOC.*, 1987, pp. 218-229.

[21] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Nat. Comput. Conf.*, New York, USA, 1979, pp. 313-317.

[22] A. Castiglione, A. D. Santis, B. Masucci, F. Palmieri, A. Castiglione, J. Li, X. Huang, "Hierarchical and shared access control," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 4, pp. 850-865, 2015.

[23] T. Bhattacharjee, S. P. Maity and S. R. Islam, "Hierarchical secret image sharing scheme in compressed sensing," *Signal Process.: Image Commun.*, vol. 61, pp. 21-32, 2018.

[24] J. Yang and F. Fu, "New dynamic and verifiable multi-secret sharing schemes based on LFSR public key cryptosystem," *IET Inf. Secur.*, vol. 14, no. 6, pp. 783-790, Nov. 2020.