


<b>ITC 2/50</b> Information Technology and Control Vol. 50 / No. 2 / 2021 pp. 236-246 DOI 10.5755/j01.itc.50.2.27789	<b>A New Multi-stage Secret Sharing Scheme for Hierarchical Access          Structure with Existential Quantifier</b>	
	Received 2020/10/05	Accepted after revision 2021/04/07
	 <a href="http://dx.doi.org/10.5755/j01.itc.50.2.27789">http://dx.doi.org/10.5755/j01.itc.50.2.27789</a>	

**HOW TO CITE:** Xu, G., Yuan, J., Xu, G., Jia, X. (2021). A New Multi-stage Secret Sharing Scheme for Hierarchical Access Structure with Existential Quantifier. *Information Technology and Control*, 50(2), 236-246. <https://doi.org/10.5755/j01.itc.50.2.27789>

# A New Multi-stage Secret Sharing Scheme for Hierarchical Access Structure with Existential Quantifier

**Guoai Xu, Jiangtao Yuan, Guosheng Xu**

National Engineering Laboratory of Mobile Network Security, College of Cyberspace Security; Beijing University of Posts and Telecommunications; Beijing, China

**Xingxing Jia**

School of Mathematics and Statistics; Lanzhou University; Lanzhou, China

Corresponding authors: [jiangt\\_yuan@163.com](mailto:jiangt_yuan@163.com) and [jiaxx@lzu.edu.cn](mailto:jiaxx@lzu.edu.cn)

Multi-stage secret sharing scheme is practical in the case that there is a security system with  $m$  ordered checkpoints. It is natural to divide the  $m$  checkpoints into  $m$  different levels. There are  $m$  different secrets, and each of them with a different importance corresponds to a checkpoint/level. The participants are also divided into  $m$  disjoint levels as they do in the hierarchical threshold access structure. Hierarchical threshold access structure with the existential quantifier ( $HTAS_{\exists}$ ) does not cover the common practice that at least a few numbers of high-ranking participants are required to be involved in any recovery of the secret. The popular schemes with hierarchical access structure were needed to check many matrices for non-singularity. We propose a multi-stage secret sharing scheme for  $HTAS_{\exists}$ , and the tools are based on the linear homogeneous recurrence relations (LHRRs) and one-way functions. We give the  $HTAS_{\exists}$  a modification, so that this hierarchical access structure can satisfy the common practice. In our scheme, if the participants are divided into  $m$  levels, there usually has  $m$  secrets. But before the  $(j - 1)$ -th secret is recovered, the  $j$ -th secret cannot be recovered. Our scheme is a computational secure. The proposed scheme requires a share for each participant and the share is as long as each secret. Our scheme has high efficiency by comparing with the state-of-the-art hierarchical secret sharing schemes.

**KEYWORDS:** Hierarchical access structure, linear homogeneous recurrence relations, multi-stage, secret sharing, existential quantifier.

## 1. Introduction

In a  $(t, n)$  threshold secret sharing scheme, the secret can be shared among  $n$  participants, and any  $t$  or more participants can obtain a qualified subset to recover the shared secrets by pooling their shares. If the participants of any unqualified subset cannot obtain any information about the shared secrets, then such scheme is called as the *perfect scheme*. The threshold secret sharing schemes proposed by Shamir [25] and Blakley [2] are two special cases where all the participants have the same authorities. Such threshold secret sharing schemes are restrictive in practice. Therefore, the schemes based on different access structure were proposed [3, 22].

Hence, in order to improve the practicality of secret sharing, many researchers have focused on specific families of access structures, for example, bipartite access structures [22], compartmented access structure and hierarchical access structure [28]. Simmons proposed a multipartite access structure [26] and he gave the definition of the compartmented access structure and the hierarchical access structure. In these access structures, participants are divided into different levels, i.e., the participants have different authorities in the different levels, but the participants in the same level have the same role. After Simmons, Brickell proposed a method to construct an ideal secret sharing scheme for the multilevel and compartmented access structures [4], but the scheme is not efficient, for the exponential operations required to get nonsingular matrices. The definition of hierarchical access structure in [26] is as follows.

**Definition 1.** Let  $P$  denote the set of the participants, where  $n = |P|$ . The set  $P$  is divided into disjoint levels  $\gamma_1, \gamma_2, \dots, \gamma_m$  of the participants,  $P = \bigcup_{i=1}^m \gamma_i$  and  $\gamma_i \cap \gamma_j = \emptyset$  for all  $i \neq j$ . The level  $i$  contains  $n_i$  participants, where  $i \in \{1, 2, \dots, m\}$ . Let  $K = \{k_i\}_{i=1}^m$  be assorted in ascending order,  $0 = k_0 < k_1 < \dots < k_m$ . The  $(K; n)$ -hierarchical threshold access structure is

$$AS = \{A \subset P \mid \exists i \in \{1, 2, \dots, m\} \text{ for which} \\ |A \cap (\bigcup_{j=1}^i \gamma_j)| \geq k_i\}. \quad (1)$$

However, Tassa [27] pointed out that the common practice needed at least a few numbers of high-ranking participants to be involved in any recovery of the

secret, even though high-ranking participants could be replaced by low-ranking participants. Therefore, a different definition of the hierarchical access structure was given by the replacement of the existential quantifier  $\exists$  in (1) with the universal quantifier  $\forall$ . Later, scholars studied the hierarchical access structure with some other methods [7, 10, 11, 12, 13, 14], but these schemes were not efficient or just gave a comprehensive characterization of the ideal multipartite access structures. But the definition (1) is very practical in a multi-stage secret sharing scheme, because if  $\exists i < m$  satisfies (1), a qualified subset can recover from the first to the  $i$ -th secret. If we change the definition (1) into (2), the problem pointed out by Tassa can be avoided. We just need to set  $t_i > k_i - k_{i-1}$ . For example, set  $t_1 > k_1 - k_0 = k_1$ , i.e., just only participants from  $\gamma_1$  cannot recover the first secret, and a few numbers of high-ranking participants from  $\bigcup_{i=2}^m \gamma_i$  are required ( $t_1 - k_1$  participants are required from  $\bigcup_{i=2}^m \gamma_i$ ), where  $t_1$  is the threshold in the first stage. The detail of definition (2) can be found in preliminary and the modified definition is as follows.

$$AS' = \{A \subset P \mid \exists i \in \{1, 2, \dots, m\} \text{ for which} \\ |A \cap (\bigcup_{j=1}^i \gamma_j)| \geq k_i \text{ and } t_i \geq k_i - k_{i-1} \text{ and} \\ |A - (\bigcup_{j=1}^i \gamma_j)| \geq t_i - (k_i - k_{i-1})\}. \quad (2)$$

Multi-secret sharing is a generalization of secret sharing. There are two different types multi-secret sharing schemes. The first type is that the secrets are recovered at the same time [9, 19, 29]. The second type is that for the different importance of different secrets, these secrets are recovered in a different stage [5, 15, 17, 18, 21], i.e., the qualified subset can recover only one secret in each stage. Our scheme belongs to the second type, and the order of these secret are determined by the distributor. In 1994, He et al. [18] proposed a multi-stage secret sharing scheme based on one-way function. Later, Harn [17] gave a modification on [18] and proposed a scheme with  $k(n-t)$  public values, which had fewer public values than He et al.'s scheme. Chang et al. [5] pointed out that the two schemes [17-18] have the same shortcomings that these secrets cannot be recovered in the order that was determined by the distributor. For a multi-stage secret sharing scheme, the participants should show the combiners the pseudo shares depending on

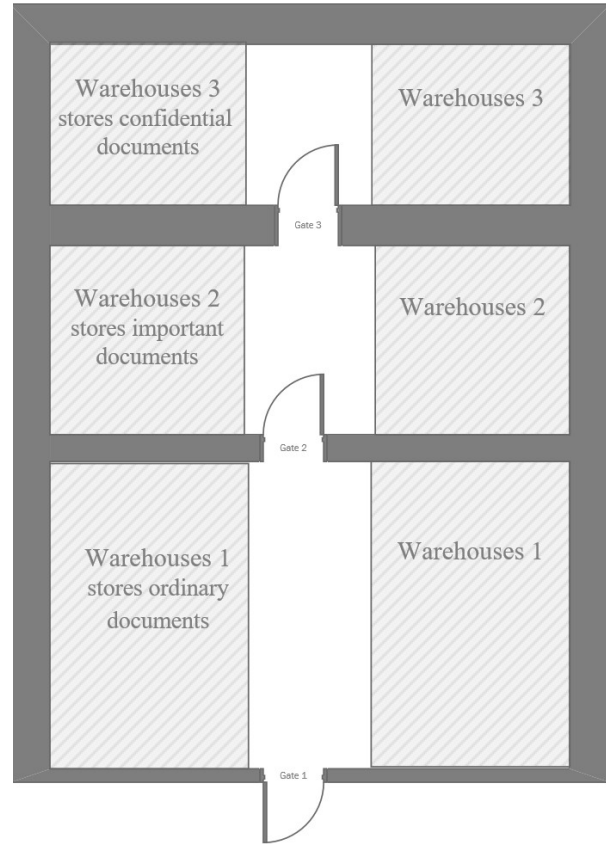
the shadows (original shares). So the multi-stage secret sharing scheme are usually based on the one-way function [5, 17, 18] or the factorization problem [28]. In the cryptographic system, the application of multi-stage secret sharing scheme is very useful in the lattice [23]. A multi-secret sharing scheme is claimed as multi-stage, if the recovered secrets can not leak any information about the unrecovered secrets. For this purpose, two security requirements are needed:

- 1 Each participant's shadow should be masked by the pseudo-shares during the recovery phase.
- 2 The recovery of a secret should not endanger another unrecovered secret.

In some firms or government services, the situation that different important things are stored in different warehouses may come up. For example, there are three warehouses to store ordinary files, important documents and confidential documents, respectively, i.e., the warehouse that store confidential documents has the highest security level. Fig.1 show the order of three different warehouses. If some employees want to get the ordinary files, they are not allowed to get all the three secrets, but have the secret of warehouse 1. If the qualified participants want to open the warehouse 2, the warehouse 1 must be opened firstly, i.e., the qualified participants should recover two secrets, the first secret of warehouse 1 and the second secret of warehouse 2. The participants of a qualified subset do not have to open all the warehouses. The stuff that are stored in the warehouse 2 are more important than these stuff that are stored in the warehouse 1. Therefore, the secret corresponding to the warehouse 2 is more important than the secret corresponding to the warehouse 1. In this situation, the employees are divided into three disjoint levels  $\gamma'_1, \gamma'_2, \gamma'_3$ . The participants in  $\gamma'_1$  just can recover the secret of warehouse 1 and the participants in  $\gamma'_2$  can recover the secrets of warehouse 1 and warehouse 2, and so on. If we want to satisfy the common practice pointed out by Tassa [27], when the participants in  $\gamma'_1$  want to recover the secret of warehouse 1, the participants in higher levels need to be involved in the recovery of it (the participants in higher levels belong to  $\bigcup_{i=2}^3 \gamma'_i$ ). But when the secret of warehouse 3 needs to be recovered, just the participants in  $\gamma'_3$  can recover it, i.e., the last secret just can be recovered by the participants in the highest level. In our scheme, the importance of the secrets is ascending, i.e.,  $key_1 < key_2 < \dots < key_m$ ,

**Figure 1**

The order of three different warehouses



where “ $<$ ” denotes that the importance is ascending. The importance of the participants in these levels is ascending too, and the participants play the same role in the same level, i.e.,  $\gamma_1 < \gamma_2 < \dots < \gamma_m$ . If there are  $m$  different checkpoints, the set  $P$  of the participants is usually divided into  $m$  disjoint levels  $\gamma_1, \gamma_2, \dots, \gamma_m$ . We call the level  $\gamma_j$  corresponding level of the secret  $key_j$ . The first secret  $key_1$  is used to open the first checkpoint and the second secret  $key_2$  is used to open the second checkpoint, and so on. The participants in the subset  $\gamma_j$  can pool the shares to recover from the first to the  $j$ -th secret.

Our scheme is motivated to give an efficient multi-stage secret sharing scheme for the hierarchical access structure with the existential quantifier  $\exists$ . If  $\exists i < m$  satisfies (2), then the participants in the qualified subset are not allowed to recover all secrets (For example, if  $\exists i = 3$  satisfies (2), the participants in the qualified subset are allowed to recover from the first to third secret). So it is natural to design a multi-stage secret sharing scheme

by using access structure with the existential quantifier  $\exists$ . When these secrets are recovered in order, it is also natural to think that the secrets are hierarchical and each secret can be recovered by the participants of the *corresponding level* and the levels that are higher than the corresponding level. Even Brickell [4] gave an ideal scheme, the scheme is inefficient and there is a shortcoming pointed out by Tassa [27] in the hierarchical access structure with the existential quantifier  $\exists$  [4, 26]. It is asserted that the participants are semi-honest and the distributor is trusty in our scheme. The proposed scheme is based on two technologies, the linear homogeneous recurrence (LHR) relations [8, 29] and the one-way functions [16, 20]. Mashhadi and Dehkordi first introduced the linear homogeneous recurrence (LHR) relations to the threshold secret sharing schemes [8]. Later, Yuan et al. introduced it to dynamic secret sharing scheme [29]. But the participants are assumed to have the equal privilege in these schemes. Our main contributions are as follows.

- 1 We give a modification of the hierarchical access structure with existential quantifier [4] and solve the problem pointed out by Tassa. The problem was that the common practice needed at least a few numbers of high-ranking participants to be involved in any recovery of the secret. We just need to set some  $t_i$ s to satisfy  $t_i > k_i - k_{i-1}$ , where  $1 \leq i < m$  and  $k_0 = 0$ .
- 2 Our scheme are more efficient than Brickell's scheme, since the exponential operations are not required for assigning identities and shares to the participants in the proposed scheme. Each participant only needs to hold a shadow during the whole scheme and each shadow is as long as the secret.

The remainder of this paper is organized as follows. Section 2 provides preliminaries of secret sharing scheme, linear homogeneous recurrence relation. Section 3 presents the proposed scheme. Section 4 shows the properties of the proposed scheme, and in this section, we also give the security analysis of our scheme and compare the existing popular works with the proposed scheme. Finally, Section 5 draws our conclusion.

## 2. Preliminary

In this section, we give a brief description of the secret sharing schemes and the LHR relations [29].

### 2.1. Secret Sharing Schemes

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

**Definition 2.** A  $(t, n)$  threshold secret sharing scheme  $\Pi : S \times R \rightarrow S_1 \times S_2 \times \dots \times S_n$  over  $P$  ( $P$  is the set of participants in the game, that is,  $P = \{P_1, P_2, \dots, P_n\}$  and  $P = |n|$ ), 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  $|A| \geq t$ ,  $H(S | S_A) = 0$ , where  $A$  is the subset of participants,  $|A|$  is the number of participants in the subset  $A$ ,  $S_A$  denotes the information of the shares to be obtained by the participants in the subset  $A$  and  $H(\cdot)$  is the function of entropy.
- 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 scheme.

In the following section, the hierarchical access structure is briefly given as follows.

**Definition 3.** Let  $P$  denote the set of the participants, where  $n = |P|$ . The set  $P$  is divided into disjoint levels  $\gamma_1, \gamma_2, \dots, \gamma_m$  of the participants,  $P = \bigcup_{i=1}^m \gamma_i$  and  $\gamma_i \cap \gamma_j = \emptyset$  for all  $i \neq j$ . The level  $i$  contains  $n_i$  participants, where  $i \in \{1, 2, \dots, m\}$ . Let  $K = \{k_i\}_{i=1}^m$  be asorted in ascending order,  $0 = k_0 < k_1 < \dots < k_m$ . The  $(K; n)$ -hierarchical threshold access structure is

$$AS' = \{A \subset P \mid \exists i \in \{1, 2, \dots, m\} \text{ for which} \\ |A \cap (\bigcup_{j=1}^i \gamma_j)| \geq k_i \text{ and } t_i \geq k_i - k_{i-1} \text{ and} \\ |A - (\bigcup_{j=1}^i \gamma_j)| \geq t_i - (k_i - k_{i-1})\} \tag{3}$$

where  $t_i$  is threshold in the  $i$ -th stage.

### 2.2. Linear Homogeneous Recurrence Relations

We give a brief description of the linear homogeneous recurrence relations. A detailed description of the linear homogeneous recurrence relations can be found in [24] [29].

**Theorem 1.** Let  $h_0, h_1, \dots, h_j, \dots$ , be a sequence of numbers and  $\alpha_1, \alpha_2, \dots, \alpha_m$  be the distinct roots of the following characteristic equation of the linear homogeneous recurrence relation with constant coefficients:

$$h_j = a_1 h_{j-1} + a_2 h_{j-2} + \dots + a_t h_{j-t}, \quad (4)$$

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

If  $\alpha_i$  is a  $s_i$ -fold root of the characteristic equation (1), then part of the general solution for this recurrence relation corresponding to  $\alpha_i$  is given as

$$\begin{aligned} F_j^{(i)} &= c_{i1} \alpha_i^j + c_{i2} j \alpha_i^j + \dots + c_{is_i} j^{s_i-1} \alpha_i^j \\ &= (c_{i1} + c_{i2} j + \dots + c_{is_i} j^{s_i-1}) \alpha_i^j. \end{aligned}$$

Let  $f_i(j) = c_{i1} + c_{i2} j + \dots + c_{is_i} j^{s_i-1}$ . We can have  $F_j^{(i)} = f_i(j) \alpha_i^j$ .

The general solution for the recurrence relation is given by

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

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

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

$$h_j = F_j, \quad (5)$$

where

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

### 3. The Proposed Scheme

This section is the main part of the paper, which shows the design of our scheme. In the section, there two phrases, i.e., construction phase and recovery phase. In our scheme, there are  $n$  participants and a trusted distributor  $D$ , and the participants are semi-honest.  $P = \{P_1, P_2, \dots, P_n\}$  denotes the  $n$  participants in the set  $P$ , where  $P_i$  is the  $i$ -th participant in  $P$ . Suppose that  $ID_i$  be the  $i$ -th participant's identity. Let the  $m$  secrets be  $key_1, key_2, \dots, key_m$  ( $m$  is the number of the disjoint subset of  $P$ ) and the importance of the secrets is ascending, i.e., the level of  $key_2$  is higher than that of

$key_1$  and so on (that is to say,  $key_1 < key_2 < \dots < key_m$ , where " $<$ " denotes the importance). Our scheme is based on the linear homogeneous recurrence relations over  $GF(q)$ , where  $GF(q)$  is a finite field, and  $q$  is a large prime.

The basic idea of our scheme is given as follows. The distributor generates  $m$  linear homogeneous recurrence relations. All the  $m$  LHR relations have two different roots. The participants in  $\gamma_1$  and  $\bigcup_{i=2}^m \gamma_i$  initialize two LHR relations, respectively, and we call them the first sub-LHR relation and the second sub-LHR relation, respectively. Then we add them. Since the sum of the general terms of two sub-LHR relations is still the general term of a LHR relation, it is called the first LHR relation (This shows how a LHR relation is generated). The participants in  $\gamma_2$  and  $\bigcup_{i=3}^m \gamma_i$  also initialize two LHR relations. According to the same method, we construct from the second to  $m$  LHR relation. The first secret  $key_1$  is hidden in the  $\max(n_1, n - n_1)$ -th term of the first LHR relation and the second secret  $key_2$  is hidden in the  $\max(n_2, n - n_1 - n_2)$ -th term of the second LHR relation, and so on. However, before the  $j$ -th  $key_j$  can be recovered, the  $(j - 1)$ -th  $key_{j-1}$  should be recovered, firstly. The Fig. 2 shows what is the construction phase in the  $j$ -th stage, where LHRR1 denotes the first sub-LHR relation, LHRR2 denotes the second sub-LHR relation, LHR denotes the LHR relation, LHRRs denotes the two sub-LHR relations,  $h_i^{(j0)}$  denotes the general term of the first sub-LHR relation of the  $j$ -th LHR relation,  $h_i^{(j1)}$  denotes the general term of the second sub-LHR relation of the  $j$ -th LHR relation and  $M_j = \max(|\gamma_j|, |\bigcup_{i=j+1}^m \gamma_i|)$ .

#### 3.1. Construction Phase

The distributor  $D$  performs the following steps to distribute the secrets:

- 1 The distributor  $D$  randomly chooses  $m$  different one-way functions  $g_1(), g_2(), \dots, g_m()$  and then publishes them.
- 2  $D$  randomly chooses  $n$  different shadows  $s_1, s_2, \dots, s_n \in Z_q^*$  and sends  $s_1, s_2, \dots, s_n$  to  $n$  participants in a secure channel, where the  $i$ -th participant holds  $s_i$ .
- 3 The distributor  $D$  selects  $2m$  different integers  $\alpha_1, \alpha_2, \dots, \alpha_m$  and  $\beta_1, \beta_2, \dots, \beta_m$  over  $GF(q)$  and publishes them, where each of them is nonzeron.
- 4 The  $j$ -th LHR relation is constructed as follows.

**4.1** Let  $K_j = k_j - k_{j-1}$ ,  $T_j = t_j - (k_j - k_{j-1})$  and  $M_j = \max(|\gamma_j|, |\bigcup_{i=j+1}^m \gamma_i|)$ .  $D$  chooses the values  $\alpha_j$  and  $\beta_j$  to make

$$(x - \alpha_j)^{K_j} = x^{K_j} + a_{j1}x^{K_j-1} + \dots + a_{jK_j} = 0 \quad (6)$$

and

$$(x - \beta_j)^{T_j} = x^{T_j} + b_{j1}x^{T_j-1} + \dots + b_{jT_j} = 0 \quad (7)$$

as the auxiliary functions of two LHR relations, where  $q > a_{ji}$  and  $q > b_{ji}$ ,  $1 \leq i \leq \max(K_j, T_j)$ ,  $1 \leq j \leq m$  and  $k_0 = 0$ .  $t_j$  is the threshold in the  $j$ -th stage.

**4.2** Suppose that the shadows in  $\gamma_j$  are  $s_{i_1}, s_{i_2}, \dots, s_{i_{n_j}}$ ,  $s_{i_{n_j}}$  and  $D$  computes the pseudo share  $R_k^j = g_j(s_{i_k})$ , where  $n_j$  is the number of the participants in  $\gamma_j$  and  $1 \leq k \leq n_j$ .

**4.3**  $D$  uses (6) to construct a LHR relation and the participants' shares in  $\gamma_j$  to initialize this LHR relation, and this LHR relation is called as the first sub-LHR relation of the  $j$ -th LHR relation. This sub-LHR relation is as follows.

$$\begin{cases} h_0^{(j0)} = R_1^j, h_1^{(j0)} = R_2^j, \dots, h_{K_j-1}^{(j0)} = R_{K_j}^j, \\ h_{i+K_j}^{(j0)} + a_{j1}h_{i+K_j-1}^{(j0)} + \dots + a_{jK_j}h_i^{(j0)} = 0 \end{cases} \quad i \geq 0. \quad (8)$$

**4.4**  $D$  calculates the rest  $h_i^{(j0)}$ , where  $K_j = k_j - k_{j-1} \leq i \leq n_j - 1$ .

**4.5**  $D$  computes  $y_i = R_i^j - h_{i-1}^{(j0)}$  and publishes  $y_i$ , where  $K_j < i \leq n_j$ .

**4.6** Assume that the shadows in  $\bigcup_{i=j+1}^m \gamma_i$  are  $s_{i_1}, s_{i_2}, \dots, s_{i_{N_j}}$ , respectively, and  $D$  computes the pseudo share  $I_k^j = g_j(s_{i_k})$ , where  $N_j$  denotes the number of the participants in the subset  $\bigcup_{i=j+1}^m \gamma_i$ .

**4.7**  $D$  uses (7) to construct another LHR relation and the participants' shares in  $\bigcup_{i=j+1}^m \gamma_i$  to initialize this LHR relation, and the LHR relation is called as second sub-LHR relation of the  $j$ -th LHR relation. This sub-LHR relation is as follows.

$$\begin{cases} h_0^{(j1)} = I_1^j, h_1^{(j1)} = I_2^j, \dots, h_{T_j-1}^{(j1)} = I_{T_j}^j, \\ h_{i+T_j}^{(j1)} + b_{j1}h_{i+T_j-1}^{(j1)} + \dots + b_{jT_j}h_i^{(j1)} = 0 \end{cases} \quad i \geq 0. \quad (9)$$

**4.8**  $D$  calculates the rest  $h_i^{(j1)}$ , where

$$T_j = t_j - (k_j - k_{j-1}) \leq i \leq N_j - 1.$$

**4.9**  $D$  computes  $y'_i = I_i^j - h_{i-1}^{(j1)}$  and publishes  $y'_i$ , where  $T_j < i \leq N_j$ .

**4.10** From the Theorem 1, the general term of (8) and (9) can be written as

$$h_i^{(j0)} = p_j(i)\alpha_j^i, \quad h_i^{(j1)} = q_j(i)\beta_j^i,$$

respectively, where the order of the polynomial  $p_j(i)$  is  $k_j - k_{j-1} - 1$

and the order of the polynomial  $q_j(i)$  is

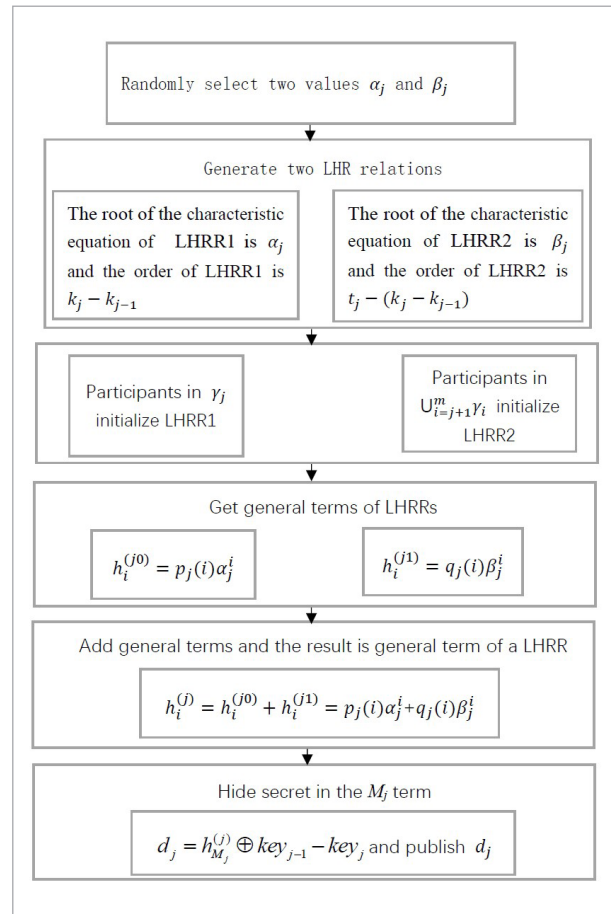
$$t_j - (k_j - k_{j-1}) - 1.$$

$h_i^{(j0)}$  and  $h_i^{(j1)}$  are the general terms of the two sub-LHR relations, respectively. Let

$$h_i^{(j)} = h_i^{(j0)} + h_i^{(j1)} = p_j(i)\alpha_j^i + q_j(i)\beta_j^i.$$

**Figure 2**

Share generation and distribution process



**Remark 1.** From the Theorem 1, we can determinate that  $h_i^{(j)}$  is the general term of a LHR relation, and we call it the  $j$ -th LHR relation. For the orders of two sub-LHR relations of the  $j$ -th relation are

$$k_j - k_{j-1} \text{ and } t_j - (k_j - k_{j-1})$$

respectively. Therefore, the order of the  $j$ -th LHR relation is

$$k_j - k_{j-1} + t_j - (k_j - k_{j-1}) = t_j.$$

We call  $t_j$  the *threshold* in the  $j$ -th stage. We name  $h_i^{(j)}$  the general term of the  $j$ -th LHR relation.

**4.11D** computes  $h_{M_j}^{(j)}$ . Then computes  $d_j = h_{M_j}^{(j)} \oplus key_{j-1} - key_j$  and publishes  $d_j$ , where  $1 \leq j \leq m$  and  $key_0 = 0$ .

**Remark 2.** From the construction, we have that if  $t_j = (k_j - k_{j-1})$ , then  $q_j(i) = 0$ . That is also to say, the participants in  $\gamma_j$  can recover the  $key_j$  without the help from the participants in the higher levels. When  $j < m$ ,  $t_j = k_j - k_{j-1}$  does not have to be satisfied. However, in the last LHR relation,  $t_j = k_j - k_{j-1}$  must satisfies, i.e.,  $q_m(i) = 0$ . That is also to say, the last secret is just shared among the participants in  $\gamma_m$ .

### 3.2. Recovery Phase

In this subsection, the process of the secret recovery would be showed. A qualified subset does not have to recover all the  $m$  secrets. Therefore, suppose that a qualified subset can recover  $i$  secrets, i.e., the participants in the qualified subset can recover these secrets from the first to the  $i$ -th secret. The process of the recovery of the  $j$ -th secret is as follows, where  $1 \leq j \leq i$ .

The  $j$ -th secret is hidden in the term  $h_{M_j}^{(j)}$  of the  $j$ -th LHR relation. Before the  $j$ -th secret can be recovered, the  $(j-1)$ -th secret  $key_{j-1}$  should be recovered. Since the order of the first sub-LHR relation of the  $j$ -th LHR relation is

$$k_j - k_{j-1}$$

and the order of the second sub-LHR relation of the  $j$ -th LHR relation is

$$t_j - (k_j - k_{j-1}),$$

the qualified subset at least contains  $t_j$  participants and  $k_j - k_{j-1}$  out of  $t_j$  are in  $\gamma_j$  ( $t_j - (k_j - k_{j-1})$  participants are from the subset  $\bigcup_{i=j+1}^m \gamma_i$ ). From the construction phase, the general term  $h_i^{(j)}$  of the first sub-

LHR relation just can be recovered by the participants from  $\gamma_j$ . The general term  $h_i^{(j)}$  of the second sub-LHR relation just can be done by the participants that are in higher level than the participants from  $\gamma_j$ , i.e., they are from  $\bigcup_{i=j+1}^m \gamma_i$ . Assume that the subset  $A \subseteq P$  satisfies the conditions. The participant  $P_i$  can get another participant  $P_j$ 's pseudo share by exchange in the qualified subset, where  $i \neq j$ . Therefore, the participants in the qualifies subset  $A$  can recover the two polynomials  $p_j(i)$  and  $q_j(i)$ , where the order of  $p_j(i)$  is

$$k_j - k_{j-1} - 1$$

and the order of  $q_j(i)$  is

$$t_j - (k_j - k_{j-1} - 1) - 1.$$

Then the participants in  $A$  can obtain the general term

$$h_i^{(j)} = p_j(i)\alpha_j^i + q_j(i)\beta_j^i = h_i^{(j0)} + h_i^{(j1)},$$

where the two values  $\alpha_j$  and  $\beta_j$  are publicly published. After the term  $h_{M_j}^{(j)}$  is obtained, the participants in  $A$  can solve the  $j$ -th secret  $key_j$  through

$$d_j = h_{M_j}^{(j)} \oplus key_{j-1} - key_j,$$

where  $d_j$  is published,  $1 \leq j \leq m$  and  $key_0 = 0$ . The two polynomials  $p_j(i)$  and  $q_j(i)$  are obtained as follows.

**Proposition 1.** If  $\alpha_i$  is a  $s_i$ -fold root of the characteristic equation (1) and the general solution for the recurrence relation (1) is given by

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

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

By exchanging the shares, the participants in the qualified subset calculate the  $k_j - k_{j-1}$  terms of the first sub-LHR relation of the  $j$ -th LHR relation, as given by:

$$h_{i-1}^{(j)} = \begin{cases} R_i^j, & 1 \leq i \leq k_j - k_{j-1} \\ R_i^j - y_i, & k_j - k_{j-1} < i \leq n_j \end{cases}. \quad (10)$$

According to Proposition 1,  $k_j - k_{j-1}$  points  $(i-1, h_{i-1}^{(j)} / \alpha_j^{i-1})$  can determinate the  $(k_j - k_{j-1} - 1)$ -th

degree polynomial  $p_j(i)$  which is defined by

$$p_j(x) = \sum_{i \in B} \frac{h_{i-1}^{(j)}}{\alpha_j^{i-1}} \prod_{\substack{j \neq i \\ j \in B}} \frac{x - j + 1}{i - j} \pmod{q} \tag{11}$$

$$= c_0 + c_1x + \dots + c_{k_{j-1}}x^{k_j - k_{j-1} - 1},$$

where  $B \in \{1, 2, \dots, n\}$ . The polynomial  $q_j(i)$  is obtained by the same the process as the polynomial  $p_j(i)$ .

### 3.3. Example

In this section, we show what are the conditions of the qualified subset and give an example to present the process of the construction phase. Suppose that the qualified subset  $A$  can recover two secrets  $key_1$  and  $key_2$ , the first secret and the second secret. Assume that there are three levels. Let  $k_1 = 3, k_2 = 5, t_1 = 5, t_2 = 4, |\gamma_1| = n_1 = 9, |\gamma_2| = n_2 = 6, |\gamma_3| = n_3 = 4, n = 19$ . That is to say,  $\gamma_1 \cup \gamma_2 \cup \gamma_3 = P$ . If  $A \in AS'$ ,  $A$  should satisfy these conditions:

$$\begin{aligned} |A \cap \gamma_1| &\geq k_1 = 3, \\ |A - \gamma_1| &\geq t_1 - (k_1 - k_0) = 2, \\ |A \cap (\gamma_1 \cup \gamma_2)| &\geq k_2 = 5, \\ |A - (\gamma_1 \cup \gamma_2)| &\geq t_2 - (k_2 - k_1) = 2. \end{aligned}$$

Thus, there are at least seven participants in  $A$ . At least three out of seven participants are from  $\gamma_1$ , at least two out of seven are from  $\gamma_2$  and at least two out of seven are from  $\gamma_3$ . The first secret is distributed as follows.

1  $D$  chooses two values  $\alpha_1, \beta_1$  and makes

$$(x - \alpha_1)^{k_1} = x^3 + a_1x^2 + a_2x + a_3 = 0 \tag{12}$$

and

$$(x - \beta_1)^{t_1 - k_1} = x^2 + b_1x + b_2 = 0 \tag{13}$$

as the auxiliary functions of two sub-LHR relations, respectively. The order of the first sub-LHR relation is three and the order of the second sub-LHR relation is two.

2 The pseudo shares of the participants in  $\gamma_1$  are used to initialize the first sub-LHR relation. The

second sub-LHR relation is initialized by these pseudo shares of the participants in  $\gamma_2 \cup \gamma_3$ . The general terms of the two sub-LHR relations are

$$h_i^{(10)} = p_1(i)\alpha_1^i, h_i^{(11)} = q_1(i)\beta_1^i,$$

respectively, where the order of  $p_1(i)$  is two and the order of  $q_1(i)$  is one.

3  $D$  adds the two general terms and let the sum

$$h_i^{(1)} = h_i^{(10)} + h_i^{(11)}$$

be the general term of the first LHR relation.

4  $D$  computes  $h_{M_1}^{(1)} = h_{10}^{(1)}$  and publishes  $d_1 = h_{10}^{(1)} \oplus key_0 - key_1$ , where  $key_0 = 0$ .

The second secret is distributed as follows.

1  $D$  chooses two values  $\alpha_2, \beta_2$  and makes

$$(x - \alpha_2)^{k_2 - k_1} = x^2 + c_1x + c_2 = 0 \tag{14}$$

and

$$(x - \beta_2)^{t_2 - (k_2 - k_1)} = x^2 + e_1x + e_2 = 0 \tag{15}$$

as the auxiliary functions of two sub-LHR relations. The order of the first sub-LHR relation is two and the order of the second sub-LHR relation is also two.

2 The pseudo shares of the participants in  $\gamma_2$  are used to initialize the first sub-LHR relation. The second sub-LHR relation is initialized by these pseudo shares of the participants in  $\gamma_3$ . The general terms of the two sub-LHR relations are

$$h_i^{(20)} = p_2(i)\alpha_2^i, h_i^{(21)} = q_2(i)\beta_2^i,$$

respectively, where the order of  $p_2(i)$  is one and the order of  $q_2(i)$  is also one.

3  $D$  adds the two general terms and let the sum

$$h_i^{(2)} = h_i^{(20)} + h_i^{(21)}$$

be the general term of the second LHR relation.

4  $D$  computes  $h_6^{(2)}$  and publishes  $d_2 = h_6^{(2)} \oplus key_1 - key_2$ .



## 4. The Properties of the Proposed Scheme

In this section, first, we give a security analysis of the proposed scheme. Then, we present the properties of our scheme.

In the below three paragraphs, we mainly give an analysis that shows why our scheme keeps secure for the unqualified subset. If the participants in an unqualified subset can recover a secret, we say that an unqualified subset can break our scheme. Since the proposed scheme is multi-stage, we just need to prove that the first secret is secure for the unqualified subset. Suppose that there are  $t_1 - 1$  participants in this unqualified subset. For the sake of simplicity, assume that the unqualified subset  $B$  contains  $k_1 - 1$  participants want to recover the general term of the first sub-LHR relation of the first LHR relation.

**Theorem 4.** The  $k_1$ -order linear homogeneous recurrence relation is secure for the unqualified participants if and only if the  $(k_1 - 1)$ -order polynomial is secure for the unqualified participants.

**Proof.** ( $\Rightarrow$ ) Suppose that the  $k_1$ -order linear homogeneous recurrence relation is secure for the unqualified participants. From (5), (8), (11) and the public value  $\alpha_1 \neq 0$ , we can get

$$h_i^{(1)} = p_1(i)\alpha_1^i \Rightarrow h_i^{(1)} / \alpha_1^i = p_1(i), \quad (16)$$

where the order of  $p_1(i)$  is  $k_1 - 1$ . From the above, we know that public value  $\alpha_1$  does not leak any information except the characteristic equation. If the  $(k_1 - 1)$ -order polynomial is not secure for the unqualified participants, i.e., the  $k_1 - 1$  points can determine a  $(k_1 - 1)$ -order polynomial. From (16), we also infer that the  $k_1 - 1$  values can determine the linear homogeneous recurrence relation with  $k_1$  order. This is contradictory to Proposition 1.

( $\Leftarrow$ ) Suppose that the  $(k_1 - 1)$ -order polynomial is secure for the unqualified participants. If the  $k_1$ -order linear homogeneous recurrence relation is not secure for the unqualified participants, then  $k_1 - 1$  random terms  $(h_{i_1}^{(1)}, h_{i_2}^{(1)}, \dots, h_{i_{k_1-1}}^{(1)})$  can determine the linear homogeneous recurrence sequences. According to (16), so we pick up  $k_1 - 1$  different terms and then can get  $k_1 - 1$  points of the polynomial  $p_1(i)$ . Since the number of the roots of the  $p_1(i)$  is  $k_1 - 1$  at most in the

field  $F$ , we can say that  $k_1 - 1$  points can determine a  $(k_1 - 1)$ -order polynomial. This is contradictory to our assumption. So the problem whether the participants from the unqualified subset  $B$  satisfying the above conditions can recover the first LHR relation can be seen as the problem that  $k_1 - 1$  points can determine the  $(k_1 - 1)$ -order polynomial.

However, there is another case that a qualified subset wants to recover other secrets which are unqualified for them. For example, the subset  $B$  can recover from the first to  $j$ -th secret, but they want to recover the  $(j+1)$ -th and the  $(j+2)$ -th secret. We can infer that from the above proof, it is impossible, and the proof is as same as the above. But in the recovery phase, the participants exchange the pseudo shares. We can conclude that the probability of breaking our scheme is not greater than the probability of breaking the one-way function. Thus, we can say that our scheme is secure. ■

### 4.1. Performance

In our scheme, each participant just holds a shadow to share one secret or more than one secrets in the whole recovery process, because in the  $j$ -th stage, participant  $P_i$  use the one-way function to generate his/her pseudo share  $g_j(s_i)$  to construct the LHR relation, i.e., the participant  $P_i$  just holds the shadow  $s_i$  during the whole process. The shadow is as long as a secret.

If  $t_i$  is set as  $t_i = k_i - k_{i-1}$ , then  $|A - \bigcup_{j=1}^i \gamma_j| \geq t_i - (k_i - k_{i-1}) \geq 0 \Rightarrow AS' = AS$ . So disjunctive access structure (1) is a trivial disjunctive access structure of (2). When  $t_i = k_i - k_{i-1}$ , we can determine  $AS' = AS$ . But when  $t_i > k_i - k_{i-1}$  from (2), we know  $|A - \bigcup_{j=1}^i \gamma_j| \geq t_i - (k_i - k_{i-1}) \geq 1$ ,  $1 \leq i < m$ . While a secret can be recovered, except the last secret, a mini number of the participants whose corresponding level is higher than this secret should be involved. Therefore, when  $t_i$  is sent as  $t_i > k_i - k_{i-1}$  ( $1 \leq i < m$ ), the problem pointed out by Tassa [8] can be solved (when  $i = m$ ,  $t_i = k_i - k_{i-1}$ , i.e., the last secret just can be recovered from the highest participants in  $\gamma_m$ ).

### 4.2. Efficiency

In this paragraph, we discuss the efficiency of our scheme and give comparisons between the existing popular works [7, 27] with our scheme. The computational complexity of the proposed scheme mainly

**Table 1**

Comparing the existing popular works with our scheme

Schemes	Tassa [27]	Chen et al. [7]	Our scheme
Approach	Polynomial derivatives	Integer polymatroids and Brickells method [4]	LHR relations
The most time cost for calculation	Assigning identities and shares to the participants	Finding nonsingular matrices	Generating or recovering LHR relations
Time cost	Exponential time	Exponential time	Polynomial time
Security	Perfect	Perfect	Computational ecurity

depends on the orders of the  $m$  generating LHR relations, and the order of the  $i$ -th LHR relation is  $t_i$ . From Theorem 1, if the public values  $\alpha_i, \beta_i$  are constant values, the computational complexity of these values is  $O(\log n)$ . So the computational complexity of the LHR relation with the order  $t_i$  is  $O(n^{\max(t_i-1)} \log n)$ , where  $1 \leq i \leq m$ . From the above security analysis, the security of our scheme has nothing to do with the public values  $\alpha_i, \beta_i$ . For reducing the computational complexity of the proposed scheme, the  $D$  usually selects the special values (like the values 1, -1, 2, ...). The space complexity of the proposed scheme mainly depends on the public values and the  $m$  public one-way functions  $g_i(\cdot)$ , where  $1 \leq i \leq m$ . From the construction phase, the number of the public values is  $mn - ((m-2)n_1 + (m-3)n_2 + \dots + n_m) + 3m - \sum_{i=1}^m t_i$ . In the next of this paragraph, we make the comparisons Tassa [27] and Chen et al. [7] with our scheme. Table 1 shows the comparisons.

From the Table 1, our scheme is computationally efficient than the existing popular works [7, 28]. Even though it may be unfair or meaningless to compare the perfect scheme with the scheme of the computational security, these schemes with computational security are useful, when a weaker security can satisfy the practice and it is hard to find an efficient and perfect scheme. Even though there has more public

values in the proposed scheme, our scheme is more efficient than the existing popular schemes.

## 5. Conclusion

Based on the linear homogeneous recurrence relations and one-way functions, we propose a multi-stage secret sharing scheme for the hierarchical access structure with the existential quantifier. Each participant just holds only a shadow during the whole scheme and the shadow is as long as the secret.

Our scheme overcomes the drawbacks that the distributor must perform possibly exponentially many checks when assigning identities and shares to the participants, if the schemes are based on Birkhoff interpolation. The proposed scheme also overcomes the drawbacks of Chen et al.'s scheme in which many matrices for non-singularity should be checked. Our scheme solves the problem pointed out by Tassa through setting  $t_i > k_i - k_{i-1}$ , where  $1 \leq i < m$ . In the future, we will try to design a perfect hierarchical secret sharing scheme Based on the LHR relations.

## Acknowledgement

This work was supported by the National Key Research and Development Program of China under Grant 2018YFB0803605.

## References

- Bhattacharjee, T., Maity, S. P., Islam, S. R. Hierarchical Secret Image Sharing Scheme in Compressed Sensing. *Signal Processing: Image Communication*, 2018, 61, 21-32. <https://doi.org/10.1016/j.image.2017.10.012>
- Blakley, G. R. Safeguarding Cryptographic Keys. In *International Work-shop on Managing Requirements Knowledge (MARK)*, IEEE, 1979, 48, 313-317. <https://doi.org/10.1109/MARK.1979.8817296>
- Blundo, C., De Santis, A., Stinson, D. R., Vaccaro, U. Graph Decompositions and Secret Sharing Schemes. *Journal of Cryptology*, 1995, 8(1), 39-64. <https://doi.org/10.1007/BF00204801>

4. Brickell, E. F. Some Ideal Secret Sharing Schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 1989, 9, 468-475. [https://doi.org/10.1007/3-540-46885-4\\_45](https://doi.org/10.1007/3-540-46885-4_45)
5. Chang, T. Y., Hwang, M. S., Yang, W. P. A New Multistage Secret Sharing Scheme Using One-Way Function. *ACM SIGOPS Operating Systems Review*, 2005, 39, 48-55. <https://doi.org/10.1145/1044552.1044557>
6. Chang, T. Y., Hwang, M. S., Yang, W. P. An Improved Multistage Secret Sharing Scheme Based on the Factorization Problem. *Information Technology and Control*, 2011, 40, 246-251. <https://doi.org/10.5755/j01.itc.40.3.633>
7. Chen, Q., Tang, C., Lin, Z. Efficient Explicit Constructions of Multipartite Secret Sharing Schemes. *ASIACRYPT*, 2019, 11922, 505-536. [https://doi.org/10.1007/978-3-030-34621-8\\_18](https://doi.org/10.1007/978-3-030-34621-8_18)
8. Dehkordi, M. H., Mashhadi, S. New Efficient and Practical Verifiable Multi-secret Sharing Schemes. *Information Sciences*, 2008, 178, 2262-2274. <https://doi.org/10.1016/j.ins.2007.11.031>
9. Endurthi, A., Chanu, O. B., Tentu, A. N., Venkaiah, V. C. Reusable Multi-stage Multi-secret Sharing Schemes Based on CRT. *Journal of Communications Software and Systems*, 2015, 11(1), 15-24. <https://doi.org/10.24138/jcomss.v11i1.113>
10. Farràs, O., Martí-Farré, J., Padró, C. Ideal Multipartite Secret Sharing Schemes. *EUROCRYPT*, Springer-Verlag, 2007, 448-465. [https://doi.org/10.1007/978-3-540-72540-4\\_26](https://doi.org/10.1007/978-3-540-72540-4_26)
11. Farràs, O., Martí-Farré, J., Padró, C. Ideal Multipartite Secret Sharing Schemes. *Journal of Cryptology*, 2012, 25, 434-463. <https://doi.org/10.1007/s00145-011-9101-6>
12. Farràs, O., Padró, C. Extending Brickell-Davenport Theorem to Non-perfect Secret Sharing Schemes. *Designs, Codes and Cryptography*, 2015, 2, 495-510. <https://doi.org/10.1007/s10623-013-9858-8>
13. Farràs, O., Padró, C. Ideal Hierarchical Secret Sharing Schemes. *IEEE Transactions on Information Theory*, 2012, 58, 3273-3286. <https://doi.org/10.1109/TIT.2011.2182034>
14. Farràs, O., Padró, C., Chaoping, X., An, Y. Natural Generalizations of Threshold Secret Sharing. *IEEE Transactions on Information Theory*, 2014, 3, 1652-1664. <https://doi.org/10.1109/TIT.2014.2300113>
15. Fatemi, M., Eghlidos, T. T., Aref, M. A Multi-stage Secret Sharing Scheme Using All-or-Nothing Transform Approach. *Proceedings of the 11th International Conference on Information and Communications Security*, Springer Berlin Heidelberg, 2009. [https://doi.org/10.1007/978-3-642-11145-7\\_35](https://doi.org/10.1007/978-3-642-11145-7_35)
16. Goldreich, O., Micali, S., Wigderson, A. How to Play Any Mental Game or a Completeness Theorem for Protocols with Honest Majority. *STOC*, 1987. <https://doi.org/10.1145/28395.28420>
17. Ham, L. Comment: Multistage Secret Sharing Based on One-way Function. *Electronics Letters*, 1995, 31(4), 262. <https://doi.org/10.1049/el:19950201>
18. He, J., Dawson, E. Multistage Secret Sharing Based on One-way Function. *Electronics Letters*, 1994, 30(19), 1591-1592. <https://doi.org/10.1049/el:19941076>
19. Herranz, J., Ruiz, A., Sáez, G. New Results and Applications for Multi-secret Sharing Schemes. *Designs, Codes and Cryptography*, 2014, 73(3), 841-864. <https://doi.org/10.1007/s10623-013-9831-6>
20. Hung-Min, S. On-line Multiple Secret Sharing Based on a One-way Function. *Computer Communications*, 1999, 8. [https://doi.org/10.1016/S0140-3664\(99\)00037-7](https://doi.org/10.1016/S0140-3664(99)00037-7)
21. Li, H. X., Cheng, C. T., Pang, L. J. An Improved Multistage (t, n) Threshold Secret Sharing Scheme. *International Conference on Advances in Web-age Information Management*. Springer-Verlag, 2005. [https://doi.org/10.1007/11563952\\_24](https://doi.org/10.1007/11563952_24)
22. Padro, C., Sez, G. Secret Sharing Schemes with Bipartite Access Structure. *IEEE Transactions on Information Theory*, 2000, 46, 2596-2604. <https://doi.org/10.1109/18.887867>
23. Píllaram, H., Eghlidos, T. An Efficient Lattice Based Multi-stage Secret Sharing Scheme. *IEEE Transactions on Dependable and Secure Computing*, 2015, 14, 2-8. <https://doi.org/10.1109/TDSC.2015.2432800>
24. Richard, B. A. *Introductory Combinatorics*, 5th ed., China Machine Press, 2009.
25. Shamir, A. How to Share a Secret. *Communications of the ACM*, 1979, 22(11), 612-613. <https://doi.org/10.1145/359168.359176>
26. Simmons, G. J. How to (Really) Share a Secret. *Conference on the Theory and Application of Cryptography*. Springer, New York, NY, 1988, 390-448. [https://doi.org/10.1007/0-387-34799-2\\_30](https://doi.org/10.1007/0-387-34799-2_30)
27. Tassa, T. Hierarchical Threshold Secret Sharing. *Journal of Cryptology*, 2007, 20, 237-264. <https://doi.org/10.1007/s00145-006-0334-8>
28. Tassa, T., Dyn, N. Multipartite Secret Sharing by Bivariate Interpolation. *Journal of Cryptology*, 2009, 22(2), 227-258. <https://doi.org/10.1007/s00145-008-9027-9>
29. Yuan, J., Li, L. A Fully Dynamic Secret Sharing Scheme. *Information Sciences*, 2019 496, 42-52. <https://doi.org/10.1016/j.ins.2019.04.061>

