Efficient Explicit Constructions of Multipartite Secret Sharing Schemes

Qi Chen[1(✉)], Chunming Tang[2], and Zhiqiang Lin[2]

[1] Advanced Institute of Engineering Science for Intelligent Manufacturing, Guangzhou University, Guangzhou 510006, China
chenqi.math@gmail.com

[2] College of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China
ctang@gzhu.edu.cn, linzhiqiang0824@163.com

Abstract. Multipartite secret sharing schemes are those having a multipartite access structure, in which the set of participants is divided into several parts and all participants in the same part play an equivalent role. Secret sharing schemes for multipartite access structures have received considerable attention due to the fact that multipartite secret sharing can be seen as a natural and useful generalization of threshold secret sharing.

This work deals with efficient and explicit constructions of ideal multipartite secret sharing schemes, while most of the known constructions are either inefficient or randomized. Most ideal multipartite secret sharing schemes in the literature can be classified as either hierarchical or compartmented. The main results are the constructions for ideal hierarchical access structures, a family that contains every ideal hierarchical access structure as a particular case such as the disjunctive hierarchical threshold access structure and the conjunctive hierarchical threshold access structure, and the constructions for compartmented access structures with upper bounds and compartmented access structures with lower bounds, two families of compartmented access structures.

On the basis of the relationship between multipartite secret sharing schemes, polymatroids, and matroids, the problem of how to construct a scheme realizing a multipartite access structure can be transformed to the problem of how to find a representation of a matroid from a presentation of its associated polymatroid. In this paper, we give efficient algorithms to find representations of the matroids associated to the three families of multipartite access structures. More precisely, based on know results about integer polymatroids, for each of the three families of access structures, we give an efficient method to find a representation of the integer polymatroid over some finite field, and then over some finite extension of that field, we give an efficient method to find a presentation of the matroid associated to the integer polymatroid. Finally, we construct ideal linear schemes realizing the three families of multipartite access structures by efficient methods.

Keywords: Secret sharing schemes · Multipartite access structures · Matroids · Polymatroids

S. D. Galbraith and S. Moriai (Eds.): ASIACRYPT 2019, LNCS 11922, pp. 505–536, 2019.
https://doi.org/10.1007/978-3-030-34621-8_18

1 Introduction

Secret sharing is an important cryptographic primitive, by means of which a secret value is distributed into shares among a number of participants in such a way that only the qualified sets of participants can recover the secret value from their shares. A scheme is *perfect* if the unqualified subsets do not obtain any information about the secret. The first proposed secret sharing schemes [8,31] realized *threshold access structures*, in which the qualified subsets are those having at least a given number of participants. In addition, these schemes are *ideal* and *linear*. A scheme is ideal if the share of every participant has the same length as the secret, and it is linear if the linear combination of the shares of different secrets results in shares for the same linear combination of the secret values. Even though there exists a linear secret sharing scheme for every access structure [6,24], the known general constructions are not impractical because the length of the shares grows exponentially with the number of participants. Actually, the optimization of secret sharing schemes for general access structures has appeared to be an extremely difficult problem and not much is known about it. Nevertheless, secret sharing schemes have found numerous applications in cryptography and distributed computing, such as threshold cryptography [16], secure multiparty computations [5,11,14,15], and oblivious transfer [32,36]. In many of the applications mentioned above, we hope to use practical schemes, namely, the linear schemes in which the size of the share of each participant is a polynomial of the size of the secret. In particular, we want to use the ideal schemes since they are the most space-efficient.

Due to the difficulty of constructing an ideal liner scheme for every given access structure, it is worthwhile to find families of access structures that admit ideal linear schemes and have useful properties for the applications of secret sharing. Several such families are formed by multipartite access structures, in which the set of participants is divided into different parts and all participants in the same part play an equivalent role. Weighted threshold access structures [4,31], hierarchical access structures [18,34,35], and compartmented access structures [9,22,37] are typical examples of such multipartite access structures. Readers can refer to [19] for comprehensive survey on multipartite access structures. A great deal of the ongoing research in this area is devoted to the properties of multipartite access structures and to secret sharing schemes (especially ideal and linear ones) that realize them.

The first class of multipartite access structures is weighted threshold access structures which appeared in the seminal paper by Shamir [31]. Weighted threshold access structures do not admit an ideal secret sharing scheme in general. Ideal multipartite secret sharing and their access structures were initially studied by Kothari [25] and by Simmons [34]. Kothari [25] presented some ideas to construct ideal linear schemes with hierarchical properties. Simmons [34] introduced the multilevel access structures (also called disjunctive hierarchical threshold access structures (DHTASs) in [35]) and compartmented access structures, and constructed ideal linear schemes for some of them by geometric method [8], but the method is inefficient. The efficient method to construct ideal linear schemes

for DHTASs was presented by Brickell [9] based on primitive polynomials over finite fields. He also presented a more general family, that is the so-called compartmented access structures with lower bounds (LCASs) as a generalization of Simmons' compartmented access structures and offered a method to construct ideal linear schemes realizing LCASs too. This method is efficient to construct schemes realizing Simmons' compartmented access structures but is inefficient to construct the schemes realizing LCASs in general because it is required to check (possible exponentially) many matrices for non-singularity. Tassa [35] presented conjunctive hierarchical threshold access structures (CHTASs) and offered a method to construct ideal linear schemes realizing them based on Birkhoff interpolation. In the case of random allocation of participant identities, this method is probabilistic. A method is probabilistic if it produces a scheme for the given access structure with high probability. In the probabilistic method, it is still required to check many matrices for non-singularity. In general, we hope to construct schemes by efficient methods. By allocating participant identities in a monotone way, Tassa gave an efficient method to construct ideal linear schemes for CHTASs over a sufficiently large prime field based on Birkhoff interpolation. Tassa and Dyn [37] presented compartmented access structures with upper bounds (UCASs) and offered probabilistic methods to construct ideal linear schemes for UCASs, LCASs and CHTASs based on bivariate interpolation.

Another related line of work deals with the characterization of the ideal multipartite secret sharing schemes and their access structures. This line of research was initiated by Brickell [9] and by Brickell and Davenport [10]. They introduced the relationship between secret sharing schemes and matroids, and characterized the ideal secret sharing schemes by matroids. Beimel et al. [4] characterized ideal weighted threshold secret sharing schemes by matroids. The bipartite access structures were characterized in [29] and some partial results about the tripartite case were presented in [13] and [22]. On the basis of the works in [9,10], Farràs et al. [17–19] introduced integer polymatroids for the study of ideal multipartite secret sharing schemes. They studied the connection of multipartite secret sharing schemes, matroids and polymatroids, and presented many new families of multipartite access structures such as ideal hierarchical access structures (IHASs) and compartmented access structures with upper and lower bounds. Their work implies the problem of how to construct a scheme realizing a multipartite access structure can be transformed to the problem of how to find a representation of a matroid from a presentation of its associated polymatroid. Nevertheless, Farràs et al. [17,19] pointed out it remains open whether or not exist efficient algorithms to obtain representations of matroids from representations of their associated polymatroids in general.

1.1 Related Work

Efficient Explicit Constructions of Ideal Multipartite Secret Sharing. The most of the known constructions of ideal multipartite secret sharing schemes are either inefficient or randomized in the literature. Efficient methods to construct ideal hierarchical secret sharing schemes were given by Brickell [9] and by

Tassa [35]. Brickell's construction provides a representation of a matroid associated to DHTASs over finite fields of the form $\mathbb{F}_{q^\lambda}$ with $\lambda \geq mk^2$, where q is a prime power, m is the number of parts that the set of participants is divided into, and k is the rank of the matroid. An irreducible polynomial of degree λ over $\mathbb{F}_q$ has to be found, but this can be done in time polynomial in q and λ by using the algorithm given by Shoup [33]. Therefore, a representation can be found in time polynomial in the size of the ground set. Accordingly, ideal linear schemes realizing DHTASs can be obtained by an efficient method. Tassa [35] offered a representation of a matroid associated to CHTASs over prime fields $\mathbb{F}_p$ with p larger than $2^{-k+2}(k-1)^{(k-1)/2}(k-1)!N^{(k-1)(k-2)/2}$, where k is the rank of the matroid and N is the maximum identity assigning to participants. A matrix M is the representation if some of its submatrices are nonsingular. The non-singularity of these submatrices depends on the Birkhoff interpolation. There is an efficient algorithm to solve this kind of interpolation over the prime fields $\mathbb{F}_p$, and consequently, ideal linear schemes for CHTASs can be obtained by an efficient method. Ball et al. [1] extended the methods in [9,35] and obtained two different kinds of representations of biuniform matroids, one by using a primitive element of an extension field and another one by using a large prime field. The schemes for some bipartite access structures can be obtained based on these representations. In addition, efficient methods to construct schemes for some multilevel access structures with two levels and three levels were presented in [7] and [21], respectively.

Multipartite Secret Sharing, Polymatroids and Matroids. On the basis of the connection of multipartite secret sharing schemes, matroids and polymatroids, Farràs et al. [17–19] introduced a unified method based on polymatroid techniques, which simplifies the task of determining whether a given multipartite access structures is ideal or not. In particular, they characterized ideal secret sharing schemes for hierarchical access structures in [18] by the unified method. They defined the accurate form of IHASs and showed that every ideal hierarchical access structure is of this form or it can be obtained from a structure of this form by removing some participants. Moreover, they presented a general method to construct ideal linear schemes realizing multipartite access structures. Specially, to construct a secret sharing scheme realizing a given multipartite access structure, first find an integer polymatroid associated to the access structure, then find a representation of the integer polymatroid over some finite field, and third find a representation of the matroid associated the access structure over some finite extension of the finite field based on the representation of the integer polymatroid. The result in [17] implies the matroid can be used to construct an ideal linear scheme realizing the access structure.

1.2 Our Results

In this paper, we study how to construct secret sharing schemes realizing multipartite access structures. The main results are the constructions for IHASs,

a family that contains all ideal hierarchical access structure as a particular case such as DHTASs and CHTASs, and the constructions for UCASs and LCASs, two special families of compartmented access structures. We give efficient methods to explicitly construct ideal linear schemes realizing these access structures combining the general polymatroid-based method in [17] and Brickell's method to construct ideal linear schemes for DHTASs in [9]. The ideal of our construction is described as follows.

Our method to construct multipartite schemes is closely related to the representations of the multipartite matroid associated to the given multipartite access structure. The problem of how to obtain a representation of the multipartite matroid can be transformed to find a matrix M such that its some special submatrices are nonsingular. Thus, our main goal is that providing a polynomial time algorithms to construct such a matrix M such that all the determinants of those special submatrices are nonzero over some finite fields. More precisely, we construct the matrix M with special form such that every determinant of those submatrices can be viewed as a nonzero polynomial on x of degree at most t over some finite field $\mathbb{F}_q$. Based on such a matrix M, over $\mathbb{F}_{q^\lambda}$ with $\lambda > t$, the algorithm given by Shoup [33] implies a representation of the matroid associated the given access structure can be found in time polynomial in the size of the ground set.

The idea of finding a matrix M such that the determinants of some of its submatrices are denoted by a nonzero polynomial on x comes from Brickell [9]. This is the key to find a representation of the matroid. This is related to the determinant function of matrix. To solve this question, we introduce approaches to calculate two class of matrices with special form, one can be applied to the constructions for IHASs and another one can be applied to the constructions for UCASs and LCASs.

Specifically, based on the integer polymatroids associated to the three families of multipartite access structures presented in [17–19], for each of the three families of access structures, we give an efficient method to find a representation of the integer polymatroid over some finite field, and then over some finite extension of that field, we give an efficient method to find a presentation of the matroid associated to the integer polymatroid. Accordingly, we construct ideal linear schemes for these access structures. First, we construct a $\mathbb{F}_q$-representation of an integer polymatroid that is as simple as possible. In the constructions for IHASs, the representation is constructed based on unit matrix, and in the constructions for UCASs and LCASs, the representations are constructed based on Vandermonde matrix. Second, based on the special representation for some access structure, we construct the matrix M satisfied the required conditions such that every determinant of some of its submatrices can be viewed as a nonzero polynomial on x over $\mathbb{F}_q$. Thus, a representation of the matroid associated the given access structure can be found in time polynomial in the size of the ground set by the algorithm in [33].

In addition, we compare our results with the efficient methods to construct multipartite secret sharing schemes from [9,35] in Sect. 4.3. In particular,

we point out that our construction for DHTASs is the same as the one in [9], but we improve the bound for the size of the ground set.

1.3 Organization of the Paper

Section 2 introduces some knowledge about access structures, secret sharing schemes, polymatroids, matroids, and the methods to construct secret sharing schemes by matroids and polymatroids. Section 3 introduces the approaches to calculate the determinant functions of two classes of matrices with special form. Section 4 gives two classes of constructions for ideal linear secret sharing schemes realizing IHASs. Section 5 construct ideal linear secret sharing schemes realizing UCASs and LCASs.

2 Preliminaries

We introduce here some notation that will be used all through the paper. In particular, we recall the compact and useful representation of multipartite access structures as in [17–19].

We use $\mathbb{Z}_+$ to denote the set of the non-negative integers. For every positive integer i we use the notation $[i] := \{1, \ldots, i\}$ and for every $i, j \in \mathbb{Z}_+$ we use the notation $[i, j] := \{i, \ldots, j\}$ with $i < j$. Consider a finite set J and given two vectors $\boldsymbol{u} = (u_i)_{i\in J}$ and $\boldsymbol{v} = (v_i)_{i\in J}$ in $\mathbb{Z}_+^J$, we write $\boldsymbol{u} \leq \boldsymbol{v}$ if $u_i \leq v_i$ for every $i \in J$. The *modulus* $|\boldsymbol{u}|$ of a vector $\boldsymbol{u} \in \mathbb{Z}_+^J$ is defined by $|\boldsymbol{u}| = \sum_{i\in J} u_i$. For every subset $X \subseteq J$, we notate $\boldsymbol{u}(X) = (u_i)_{i\in X} \in \mathbb{Z}_+^X$. For every positive integer m, we notate $J_m = \{1, \ldots, m\}$ and $J'_m = \{0, 1, \ldots, m\}$. Of course the vector notation that has been introduced here applies as well to $\mathbb{Z}_+^m = \mathbb{Z}_+^{J_m}$.

2.1 Access Structures and Secret Sharing Schemes

Let $P = \{p_1, \ldots, p_n\}$ denote the set of participants and its power set be denoted by $\mathcal{P}(P) = \{\mathcal{V} : \mathcal{V} \subseteq P\}$ which contains all the subsets of P. A collection $\Gamma \subseteq \mathcal{P}(P)$ is monotone if $\mathcal{V} \in \Gamma$ and $\mathcal{V} \subseteq \mathcal{W}$ imply that $\mathcal{W} \in \Gamma$. An *access structure* is a monotone collection $\Gamma \subseteq \mathcal{P}(P)$ of nonempty subsets of P. Sets in Γ are called *authorized*, and sets not in Γ are called *unauthorized*. An authorized set $\mathcal{V} \in \Gamma$ is called a *minimal authorized set* if for every $\mathcal{W} \subsetneq \mathcal{V}$, the set $\mathcal{W}$ is unauthorized. An unauthorized set $\mathcal{V} \notin \Gamma$ is called a *maximal unauthorized set* if for every $\mathcal{W} \supsetneq \mathcal{V}$, the set $\mathcal{W}$ is authorized. The set $\Gamma^* = \{\mathcal{V} : \mathcal{V}^c \notin \Gamma\}$ is called the *dual* access structure to Γ. It is easy to see that Γ^* is monotone too. In particular, an access structure is said to be *connected* if all participants are in at least one minimal authorized subset.

A family $\Pi = (\Pi_i)_{i\in J_m}$ of subsets of P is called here a *partition* of P if $P = \bigcup_{i\in J_m} \Pi_i$ and $\Pi_i \cap \Pi_j = \emptyset$ whenever $i \neq j$. For a partition Π of a set P, we consider the mapping $\Pi : \mathcal{P}(P) \to \mathbb{Z}_+^m$ defined by $\Pi(\mathcal{V}) = (|\mathcal{V} \cap \Pi_i|)_{i\in J_m}$. We write $\mathbf{P} = \Pi(\mathcal{P}(P)) = \{\boldsymbol{u} \in \mathbb{Z}_+^m : \boldsymbol{u} \leq \Pi(P)\}$. For a partition Π of a set P, a Π-*permutation* is a permutation σ on P such that $\sigma(\Pi_i) = \Pi_i$ for every part Π_i

of Π. An access structure on P is said to be Π-*partite* if every Π-permutation is an automorphism of it.

As in [17–19], we describe a multipartite access structure in a compact way by taking into account that its members are determined by the number of elements they have in each part. If an access structure Γ on P is Π-partite, then $\mathcal{V} \in \Gamma$ if and only if $\Pi(\mathcal{V}) \in \Pi(\Gamma)$. That is, Γ is completely determined by the partition Π and set of vectors $\Pi(\Gamma) \subseteq \mathbf{P} \subseteq \mathbb{Z}_+^m$. Moreover, the set $\Pi(\Gamma) \subseteq \mathbf{P}$ is monotone increasing, that is, if $\boldsymbol{u} \in \Pi(\Gamma)$ and $\boldsymbol{v} \in \mathbf{P}$ is such that $\boldsymbol{u} \leq \boldsymbol{v}$, then $\boldsymbol{v} \in \Pi(\Gamma)$. Therefore, $\Pi(\Gamma)$ is univocally determined by $\min \Pi(\Gamma)$, the family of its minimal vectors, that is, those representing the minimal qualified subsets of Γ. By an abuse of notation, we will use Γ to denote both a Π-partite access structure on P and the corresponding set $\Pi(\Gamma)$ of points in $\mathbf{P}$, and the same applies to $\min \Gamma$.

Now, we introduce some families of multipartite access structures.

Definition 1 (Ideal hierarchical access structures). *Take* $\hat{\boldsymbol{k}}, \boldsymbol{k} \in \mathbb{Z}_+^m$ *such that* $\hat{k}_1 = 0$ *and* $\hat{k}_i \leq \hat{k}_{i+1} < k_i \leq k_{i+1}$ *for* $i \in [m-1]$. *The following access structures are called* ideal hierarchical access structures (IHASs)

$$\Gamma = \{\boldsymbol{u} \in \mathbf{P} : |\boldsymbol{u}([\ell])| \geq k_\ell \text{ for some } \ell \in J_m \text{ and } |\boldsymbol{u}([i])| \geq \hat{k}_{i+1} \text{ for all } i \in [\ell-1]\}. \tag{1}$$

In particular, if $\hat{k}_i = 0$ for every $i \in J_m$ and $0 < k_1 < \cdots < k_m = k$, then IHASs is the *disjunctive hierarchical threshold access structures (DHTASs)*, which can be denoted by

$$\Gamma = \{\boldsymbol{u} \in \mathbf{P} : |\boldsymbol{u}([i])| \geq k_i \text{ for some } i \in J_m\}, \tag{2}$$

and if $0 = \hat{k}_1 < \cdots < \hat{k}_m$ and $k_1 = \cdots = k_m = k$ then IHASs is the *conjunctive hierarchical threshold access structures (CHTASs)*, which can be denoted by

$$\Gamma = \{\boldsymbol{u} \in \mathbf{P} : |\boldsymbol{u}([i])| \geq \tilde{k}_i \text{ for all } i \in J_m\}, \tag{3}$$

where $\tilde{k}_i = \hat{k}_{i+1}$ for $i \in [m-1]$ and $\tilde{k}_m = k_m$.

Definition 2 (Compartmented access structures). *Take* $\boldsymbol{t} \in \mathbb{Z}_+^m$ *and* $k \in \mathbb{N}$ *such that* $k \geq |\boldsymbol{t}|$. *The following access structures are called* compartmented access structures with lower bounds (LCASs)

$$\min \Gamma = \{\boldsymbol{u} \in \mathbf{P} : |\boldsymbol{u}| = k \text{ and } \boldsymbol{u} \geq \boldsymbol{t}\}. \tag{4}$$

Take $\boldsymbol{r} \in \mathbb{Z}_+^m$ *such that* $\boldsymbol{r} \leq \Pi(P)$ *and* $r_i \leq k \leq |\boldsymbol{r}|$ *for every* $i \in J_m$. *The following access structures are called* compartmented access structure with upper bound (UCASs)

$$\min \Gamma = \{\boldsymbol{u} \in \mathbf{P} : |\boldsymbol{u}| = k \text{ and } \boldsymbol{u} \leq \boldsymbol{r}\}. \tag{5}$$

We next present the definition of *unconditionally secure perfect secret sharing scheme* as given in [3,12]. For more information about this definition and secret sharing in general, see [2].

Definition 3 (Secret sharing schemes). *Let $P = \{p_1, \ldots, p_n\}$ be a set of participants. A* distribution scheme *$\Sigma = (\Phi, \mu)$ with domain of secrets $\mathcal{S}$ is a pair, where μ is a probability distribution on some finite set $\mathcal{R}$ called the set of random strings and Φ is a mapping from $\mathcal{S} \times \mathcal{R}$ to a set of n-tuples $\mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_n$, where $\mathcal{S}_i$ is called the domain of shares of p_i. A dealer distributes a secret $s \in \mathcal{S}$ according to Σ by first sampling a random string $r \in \mathcal{R}$ according μ, computing a vector of shares $\Phi(s, r) = (s_1, \ldots, s_n)$, and privately communicating each share s_i to participant p_i. For a set $\mathcal{V} \subseteq P$, we denote $\Phi_{\mathcal{V}}(s, r)$ as the restriction of $\Phi(s, r)$ to its $\mathcal{V}$-entries (i.e., the shares of the participants in $\mathcal{V}$).*

Let $\mathcal{S}$ be a finite set of secrets, where $\mathcal{S} \geq 2$. A distribution scheme $\Sigma = (\Phi, \mu)$ with domain of secrets $\mathcal{S}$ is a secret sharing scheme *realizing an access structure $\Gamma \subseteq \mathcal{P}(P)$ if the following two requirements hold:*

CORRECTNESS. *The secret s can be reconstructed by any authorized set of participants. That is, for any authorized set $\mathcal{V} \in \Gamma$ (where $\mathcal{V} = \{p_{i_1}, \ldots, p_{i_{|\mathcal{V}|}}\}$), there exists a reconstruction function $Recon_{\mathcal{V}} : \mathcal{S}_{i_1} \times \cdots \times \mathcal{S}_{i_{|\mathcal{V}|}} \to \mathcal{S}$ such that for every $s \in \mathcal{S}$ and every random string $r \in \mathcal{R}$,*

$$Recon_{\mathcal{V}}\big(\Phi_{\mathcal{V}}(s, r)\big) = s.$$

PRIVACY. *Every unauthorized set can learn nothing about the secret (in the information theoretic sense) from their shares. Formally, for any unauthorized set $\mathcal{W} \notin \Gamma$, every two secrets $s, s' \in \mathcal{S}$, and every possible $|\mathcal{W}|$-tuple of shares $(s_i)_{u_i \in \mathcal{W}}$,*

$$Pr\big[\Phi_{\mathcal{W}}(s, r) = (s_i)_{u_i \in \mathcal{W}}\big] = Pr\big[\Phi_{\mathcal{W}}(s', r) = (s_i)_{u_i \in \mathcal{W}}\big]$$

when the probability is over the choice of r from $\mathcal{R}$ at random according to μ.

Definition 4 (Ideal linear secret sharing schemes). *Let $P = \{p_1, \ldots, p_n\}$ be a set of participants. Let $\Sigma = (\Phi, \mu)$ be a secret sharing scheme with domain of secrets $\mathcal{S}$, where μ is a probability distribution on a set $\mathcal{R}$ and Φ is a mapping from $\mathcal{S} \times \mathcal{R}$ to $\mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_n$, where $\mathcal{S}_i$ is called the domain of shares of p_i. We say that Σ is an ideal linear secret sharing scheme over a finite field $\mathbb{K}$ if $\mathcal{S} = \mathcal{S}_1 = \cdots = \mathcal{S}_n = \mathbb{K}$, $\mathcal{R}$ is a $\mathbb{K}$-vector space, Φ is a $\mathbb{K}$-linear mapping, and μ is the uniform probability distribution.*

This paper deals with *unconditionally secure perfect ideal linear secret sharing schemes.*

2.2 Polymatroids and Matroids

In this section we introduce the definitions and some properties of polymatroids and matroids. Most results of this section are from [17–19]. For more background on matroids and polymatroids, see [23,28,30,38].

Definition 5. *A* polymatroid *$\mathcal{S}$ is defined by a pair (J, h), where J is the finite* ground set *and $h : \mathcal{P}(J) \to \mathbb{R}$ is the* rank function *that satisfies*

(1) $h(\emptyset) = 0$*;*
(2) h *is* monotone increasing*: if* $X \subseteq Y \subseteq J$*, then* $h(X) \leq h(Y)$*;*
(3) h *is* submodular*: if* $X, Y \subseteq J$*, then* $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y)$*.*

An integer polymatroid $\mathcal{Z}$ *is a polymatroid with an integer-valued rank function* h*. An integer polymatroid such that* $h(X) \leq |X|$ *for any* $X \subseteq J$ *is called a* matroid*.*

While matroids abstract some properties related to linear dependency of collections of vectors in a vector space, integer polymatroids do the same with collections of subspaces. Suppose $(V_i)_{i \in J}$ is a finite collection of subspaces of a $\mathbb{K}$-vector space V, where $\mathbb{K}$ is a finite field. The mapping $h(X) : \mathcal{P}(J) \to \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i \in X} V_i)$ is the rank function of an integer polymatroid with ground set J. Integer polymatroids and, in particular, matroids that can be defined in this way are said to be $\mathbb{K}$-*representable*.

Following the analogy with vector spaces we make the following definitions. For an integer polymatroid $\mathcal{Z}$, the set of *integer independent vectors* of $\mathcal{Z}$ is

$$\mathcal{D} = \{\boldsymbol{u} \in \mathbb{Z}_+^J : |\boldsymbol{u}(X)| \leq h(X) \text{ for every } X \subseteq J\},$$

in which the maximal integer independent vectors are called the *integer bases* of $\mathcal{Z}$. Let $\mathcal{B}$ or $\mathcal{B}(\mathcal{Z})$ denote the collection of all integer bases of $\mathcal{Z}$. Then all the elements of $\mathcal{B}(\mathcal{Z})$ have the identical modulus. In fact, every integer polymatroid $\mathcal{Z}$ is univocally determined by $\mathcal{B}(\mathcal{Z})$ since h is determined by $h(X) = \max\{|\boldsymbol{u}(X)| : \boldsymbol{u} \in \mathcal{B}(\mathcal{Z})\}$.

Given an integer polymatroid $\mathcal{Z} = (J, h)$ and a subset $X \subseteq J$, let $\mathcal{Z}|X = (X, h)$ denote a new integer polymatroid restricted $\mathcal{Z}$ on X, and $\mathcal{B}(\mathcal{Z}, X) = \{\boldsymbol{u} \in \mathcal{D} : \text{supp}(\boldsymbol{u}) \subseteq X \text{ and } |\boldsymbol{u}| = h(X)\}$ where $\text{supp}(\boldsymbol{u}) = \{i \in J : u_i \neq 0\}$. Then there is a natural bijection between $\mathcal{B}(\mathcal{Z}, X)$ and $\mathcal{B}(\mathcal{Z}|X)$.

We next introduce a class of polymatroids as follows.

Definition 6 (Boolean polymatroids). *Let* S *be a finite set and consider a family* $(S_i)_{i \in J}$ *of subsets of* S*. The mapping* $h : \mathcal{P}(J) \to \mathbb{Z}$ *defined by* $h(X) = |\bigcup_{i \in X} S_i|$ *is clearly the rank function of an integer polymatroid. Integer polymatroids that can be defined in this way are called Boolean polymatroids.*

Boolean polymatroids are very simple integer polymatroids that are representable over every finite field $\mathbb{K}$. If $|S| = t$, we can assume that S is a basis of the vector space $V = \mathbb{K}^t$. For every $i \in J$, consider the vector subspace $V_i = \langle S_i \rangle$. Obviously, these subspaces form a $\mathbb{K}$-representation of $\mathbb{Z}$.

2.3 Secret Sharing Schemes, Matroids and Polymatroids

In this section we review the methods to construct ideal linear secret sharing schemes for multipartite access structures by matroids and polymatroids. Most results of this section are from [17–19]. We first introduce the method to construct ideal linear schemes by matroids.

Let $P = \{p_1, \ldots, p_n\}$ be a set of participants and $p_0 \notin P$ be the dealer. Suppose $\mathcal{M}$ is a matroid on the finite set $P' = P \cup \{p_0\}$, and let

$$\Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P : h(A \cup \{p_0\}) = h(A)\}.$$

Then $\Gamma_{p_0}(\mathcal{M})$ is an access structure on P because monotonicity property is satisfied, which is called *the port of the matroid* $\mathcal{M}$ *at the point* p_0.

Matroid ports play a very important role in secret sharing. Brickell [9] proved that the ports of representable matroids admit ideal secret sharing schemes and provided a method to construct ideal schemes for ports of $\mathbb{K}$-representable matroids. These schemes are called a $\mathbb{K}$-*vector space secret sharing schemes*. This method was described by Massey [26,27] in terms of linear codes. Suppose M is a $k \times (n+1)$ matrix over $\mathbb{K}$. Then the columns of M determine a $\mathbb{K}$-representable matroid $\mathcal{M}$ with ground set P' such that the columns of M are in one-to-one correspondence with the elements in P'. In this situation, the matrix M is called a $\mathbb{K}$-*representation* of the matroid $\mathcal{M}$. Moreover, M is a generator matrix of some $(n+1, k)$ linear code C over $\mathbb{K}$, that is, a matrix whose rows span C. A code C of length $n+1$ and dimension k is called an $(n+1, k)$ linear code over $\mathbb{K}$ which is a k-dimensional subspace of $\mathbb{K}^{n+1}$. A secret sharing scheme can be constructed by the matrix M based the code C as follows.

Let $s \in \mathbb{K}$ be a secret value. Secret a codeword $\boldsymbol{c} = (c_0, c_1, \ldots, c_n) \in C$ uniformly at random such that $c_0 = s$, and define the share-vector as $(c_1, \ldots, c_n)$, that is c_i is the share of the participant p_i for $i \in [n]$. Let $LSSS(M)$ denote this secret sharing scheme.

Theorem 1 ([26])**.** *$LSSS(M)$ is a perfect ideal linear scheme such that a set $\mathcal{V} \subset P$ is qualified if and only if the first column in M is a linear combination of the columns with indices in $\mathcal{V}$.*

The *dual code* $C^{\perp}$ for a code C consists of all vectors $\boldsymbol{c}^{\perp} \in \mathbb{K}^{n+1}$ such that $\langle \boldsymbol{c}^{\perp}, \boldsymbol{c} \rangle = 0$ for all $\boldsymbol{c} \in C$, where $\langle \cdot, \cdot \rangle$ denotes the standard inner product. Suppose M and M^* are generator matrices of some $(n+1, k)$ linear code C and its dual $C^{\perp}$ over $\mathbb{K}$, respectively. Then $LSSS(M)$ and $LSSS(M^*)$ realize Γ and Γ^*, respectively. Sometimes it is not easy to construct an ideal linear scheme for a given access structure Γ directly. In this case we can first construct a scheme for Γ^* and then translate the scheme into an ideal linear scheme for Γ^* using the explicit transformation of [20]. In Sect. 5.2, we will present the construction for LCASs (4) by this method.

This paper deals with unconditionally secure perfect ideal linear secret sharing schemes. Brickell's method can be applied to construct such schemes. Nevertheless, it is difficult to determine whether a given access structure admits an ideal linear secret sharing scheme or not. Moreover, even for access structures that admit such schemes, it may not be easy to construct them. Some strategies based on matroids and polymatroids were presented in [17,19] to attack those problems for multipartite access structures.

The relationship between ideal multipartite access structures and integer polymatroids is summarized as follows.

Theorem 2 ([17]). *Let* $\Pi = (\Pi_i)_{i\in J_m}$ *be a partition of the set* P*, and* $\mathcal{Z}' = (J'_m, h)$ *is an integer polymatroid such that* $h(\{0\}) = 1$ *and* $h(\{i\}) \leq |\Pi_i|$ *for every* $i \in J_m$*. Take* $\Gamma_0(\mathcal{Z}') = \{X \subseteq J_m : h(X \cup \{0\}) = h(X)\}$ *and*

$$\Gamma_0(\mathcal{Z}', \Pi) = \{\boldsymbol{u} \in \mathbf{P} : \text{there exist } X \in \Gamma_0(\mathcal{Z}') \text{ and } \boldsymbol{v} \in \mathcal{B}(\mathcal{Z}'|J_m, X) \text{ such that } \boldsymbol{v} \leq \boldsymbol{u}\}.$$

Then $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$ *is a* Π*-partite access structure on* P *and a matroid port. Moreover, if* $\mathcal{Z}'$ *is* $\mathbb{K}$*-representable, then* Γ *can be realized by some* $\mathbb{L}$*-vector space secret sharing scheme over every large enough finite extension* $\mathbb{L}$ *of* $\mathbb{K}$*. In addition,* $\mathcal{Z}'$ *is univocally determined by* Γ *if it is connected.*

The general method presented by Farràs et al. [17] to construct ideal schemes for the multipartite access structures satisfying the conditions in Theorem 2 is summarized as follows.

Let $\Pi_0 = \{p_0\}$ and $\Pi' = (\Pi_i)_{i\in J'_m}$ be a partition of the set $P' = P \cup \{p_0\}$ such that $|\Pi_i| = n_i$. Given a connected Π-partite access structure Γ satisfying the conditions in Theorem 2.

Step 1. Find an integer polymatroid $\mathcal{Z}'$ such that $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$;
Step 2. Find a representation $(V_i)_{i\in J'_m}$ of $\mathcal{Z}'$ over some finite field $\mathbb{K}$;
Step 3. Over some finite extension of $\mathbb{K}$, find a representation of the matroid $\mathcal{M}$ such that Γ is a port of $\mathcal{M}$. More precisely, construct a $k \times (n+1)$ matrix $M = (M_0|M_1|\cdots|M_m)$ with the following properties:
1. $k = h(J'_m)$ and $n = \sum_{i=1}^{m} n_i$;
2. M_i is a $k \times n_i$ matrix whose columns are vectors in V_i;
3. $M_{\boldsymbol{u}}$ is nonsingular for any $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, where $M_{\boldsymbol{u}}$ is the $k \times k$ submatrix of M formed by any u_i columns in every M_i.

Farràs et al. [17–19] proved that all the multipartite access structures introduced in Sect. 2.1 are connected matroid ports. Moreover, they presented the associated integer polymatroids and proved that they are representable. Therefore, the results in [17–19] solve Step 1. In this paper, we will give an efficient method to explicitly solve Steps 2 and 3, and hence to construct ideal linear schemes for those families of access structures. Our method is based on the properties of determinant functions.

3 Some Properties of Determinant Functions

In this section, we study determinant functions of two classes of matrices with special form, which will be applied to the constructions of representations of matroids associated to multipartite access structures.

3.1 The First Class of Matrices

In this Section, we introduce the approach to calculate the determinant of a class of matrices with special form. This approach is very useful to calculate the determinant of the matrices with some zero blocks. This class of matrices will be applied to the construction of representable matroid associated to IHASs. We will use the well known Laplace Expansion Theorem of determinant.

Theorem 3 (The Laplace Expansion Theorem). *Take a $n \times n$ matrix A. Let $\boldsymbol{r} = (r_1, \ldots, r_k)$ be a list of k column indices for A such that $1 \leq r_1 < \cdots < r_k < n$ where $1 \leq k < n$ and $\boldsymbol{t} = (t_1, \ldots, t_k)$ be a list of k row indices for A such that $1 \leq t_1 < \cdots < t_k < n$ where $1 \leq k < n$. The submatrix obtained by* keeping *the entries in the intersection of any column and row that are in the lists is denoted by $S(A : \boldsymbol{r}, \boldsymbol{t})$. The submatrix obtained by* removing *the entries in the columns and rows that are in the list is denoted by $S'(A : \boldsymbol{r}, \boldsymbol{t})$. Then the determinant of A is*

$$\det(A) = (-1)^{|\boldsymbol{r}|} \sum_{\boldsymbol{t} \in \mathcal{T}} (-1)^{|\boldsymbol{t}|} \det\big(S(A : \boldsymbol{r}, \boldsymbol{t})\big) \det\big(S'(A : \boldsymbol{r}, \boldsymbol{t})\big),$$

where $\mathcal{T}$ denotes the set of all k-tuples $\boldsymbol{t} = (t_1, \ldots, t_k)$ for which $1 \leq t_1 < \cdots < t_k < n$.

Example 1. Take a 7×7 matrix $A = (A_1|A_2|A_3)$ where A_1 and A_2 are 7×2 blocks, and A_3 is a 7×3 block. Then the determinant of A can be calculated as follows.

Take $\boldsymbol{r_1} = (r_{1,1}, r_{1,2}) = (1, 2)$ and $\boldsymbol{t_1} = (t_{1,1}, t_{1,2})$. Then from Theorem 3,

$$\det(A) = (-1)^{|\boldsymbol{r_1}|} \sum_{\boldsymbol{t_1} \in \mathcal{T}_1} (-1)^{|\boldsymbol{t_1}|} \det\big(S(A : \boldsymbol{r_1}, \boldsymbol{t_1})\big) \det\big(S'(A : \boldsymbol{r_1}, \boldsymbol{t_1})\big),$$

where $\mathcal{T}_1$ denotes the set of all 2-tuples $\boldsymbol{t_1} = (t_{1,1}, t_{1,2})$ for which $1 \leq t_{1,1} < t_{1,2} \leq 7$. We proceed to calculate $\det(S'(A : \boldsymbol{r_1}, \boldsymbol{t_1}))$ by Theorem 3. Take $\boldsymbol{r_2} = (r_{2,1}, r_{2,2}) = (3, 4)$, $\boldsymbol{r} = (\boldsymbol{r_1}, \boldsymbol{r_2}) = (r_{1,1}, r_{1,2}, r_{2,1}, r_{2,2})$, $\boldsymbol{t_2} = (t_{2,1}, t_{2,2})$, $\boldsymbol{t} = (\boldsymbol{t_1}, \boldsymbol{t_2}) = (t_{1,1}, t_{1,2}, t_{2,1}, t_{2,2})$, and let $\mathcal{T}_2$ denote the set of all 2-tuples $\boldsymbol{t_2} = (t_{2,1}, t_{2,2})$ for which $1 \leq t_{2,1} < t_{2,2} \leq 7$. For a given $\boldsymbol{t_1} = (t_{1,1}, t_{1,2})$, let

$$\mathcal{T}_2(\boldsymbol{t_1}) = \mathcal{T}_2 \backslash \{(t_{2,1}, t_{2,2}) : t_{2,1} \in \{t_{1,1}, t_{1,2}\} \text{ or } t_{2,2} \in \{t_{1,1}, t_{1,2}\}\}.$$

Then

$$\det(S'(A : \boldsymbol{r_1}, \boldsymbol{t_1})) = 1)^{|\boldsymbol{r_2}|} \sum_{\boldsymbol{t_2} \in \mathcal{T}_2(\boldsymbol{t_1})} (-1)^{|\boldsymbol{t_2}|} det(S(A : \boldsymbol{r_2}, \boldsymbol{t_2})) \det(S'(A : \boldsymbol{r}, \boldsymbol{t})).$$

Hence the determinant of A can also be denoted by

$$\det(A) = (-1)^{|\boldsymbol{r}|} \sum_{\boldsymbol{t_1} \in \mathcal{T}_1} \sum_{\boldsymbol{t_2} \in \mathcal{T}_2(\boldsymbol{t_1})} (-1)^{|\boldsymbol{t}|} \det\big(S(A : \boldsymbol{r_1}, \boldsymbol{t_1})\big) \det\big(S(A : \boldsymbol{r_2}, \boldsymbol{t_2})\big) \det\big(S'(A : \boldsymbol{r}, \boldsymbol{t})\big).$$

In general, we have the following result.

Proposition 1. *Take a $n \times n$ matrix $A = (A_1| \cdots |A_m)$ where A_i is a $n \times n_i$ matrix, and take $n_0 = 0$. For every $i \in J_m$, let $\boldsymbol{r_i} = (r_{i,1}, \ldots, r_{i,n_i}) = (\sum_{j=0}^{i-1} n_j + 1, \ldots, \sum_{j=0}^{i} n_j)$, and $\boldsymbol{t_i} = (t_{i,1}, \ldots, t_{i,n_i})$ be a list of n_i row indices for A_i such that $1 \leq t_{i,1} < \cdots < t_{i,n_i} \leq n$. Take $\boldsymbol{r} = (\boldsymbol{r_1}, \ldots, \boldsymbol{r_m})$ and $\boldsymbol{t} = (\boldsymbol{t_1}, \ldots, \boldsymbol{t_m})$. Let $\mathcal{T}_i$ denote the set of all n_i-tuples $\boldsymbol{t_i} = (t_{i,1}, \ldots, t_{1,n_i})$ for which $1 \leq t_{i,1} < \cdots < t_{1,n_i} \leq n$. For a given $\boldsymbol{t_i} = (t_{i,1}, \ldots, t_{1,n_i})$, take $S(\boldsymbol{t_i}) = \{t_{i,1}, \ldots, t_{i,n_i}\}$, and for given $\boldsymbol{t_{i'}} = (t_{i',1}, \ldots, t_{i',n_{i'}})$ with $i' \in [i-1]$, take*

$$\mathcal{T}_i(\boldsymbol{t_{i'}}, i' \in [i-1]) = \mathcal{T}_i \backslash \big\{(t_{i,1}, \ldots, t_{i,n_i}) : t_{i,j} \in \bigcup_{i'=1}^{i-1} S(\boldsymbol{t_{i'}}) \text{ for some } j \in [n_i]\big\}.$$

Then

$$\det(A) = (-1)^{|\boldsymbol{r}|} \sum_{\boldsymbol{t_1} \in \mathcal{T}_1} \sum_{\boldsymbol{t_2} \in \mathcal{T}_2(\boldsymbol{t_1})} \cdots \sum_{\boldsymbol{t_{m-1}} \in \mathcal{T}_{m-1}(\boldsymbol{t_{i'}},\, i' \in [m-2])} (-1)^{|\boldsymbol{t}|} \prod_{i=1}^{m-1} \det\left(S(A : \boldsymbol{r_i}, \boldsymbol{t_i})\right) \det\left(S'(A : \boldsymbol{r}, \boldsymbol{t})\right).$$

Proof. Theorem 3 implies

$$\det(A) = (-1)^{|\boldsymbol{r_1}|} \sum_{\boldsymbol{t_1} \in \mathcal{T}_1} (-1)^{|\boldsymbol{t_1}|} \det(S(A : \boldsymbol{r_1}, \boldsymbol{t_1})) \det(S'(A : \boldsymbol{r_1}, \boldsymbol{t_1})).$$

We proceed to calculate $\det(S'(A : \boldsymbol{r_1}, \boldsymbol{t_1}))$ by Theorem 3 and the following result can be obtained

$$\det(S'(A : \boldsymbol{r_1}, \boldsymbol{t_1})) = (-1)^{|\boldsymbol{r_2}|} \sum_{\boldsymbol{t_2} \in \mathcal{T}_2(\boldsymbol{t_1})} (-1)^{|\boldsymbol{t_2}|} \det(S(A : \boldsymbol{r_2}, \boldsymbol{t_2})) \det(S'(A : (\boldsymbol{r}_1, \boldsymbol{r}_2), (\boldsymbol{t}_1, \boldsymbol{t}_2)).$$

Accordingly, $\det(S'(A : (\boldsymbol{r}_1, \ldots, \boldsymbol{r}_i), (\boldsymbol{t}_1, \ldots, \boldsymbol{t}_i)))$ can be obtained by Theorem 3 for $i \in [2, m-1]$, and the result follows. □

Example 2. Take

$$A = \left(\begin{array}{cc|cc|ccc} a_{1,1} & a_{1,2} & 0 & 0 & 0 & 0 & 0 \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & 0 & 0 & 0 \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} \\ 0 & 0 & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & a_{4,7} \\ 0 & 0 & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & a_{5,7} \\ 0 & 0 & 0 & 0 & a_{6,5} & a_{6,6} & a_{6,7} \\ 0 & 0 & 0 & 0 & a_{7,5} & a_{7,6} & a_{7,7} \end{array}\right).$$

Then from Example 1,

$$\det(A) = (-1)^{|\boldsymbol{r}|} \sum_{\boldsymbol{t_1} \in \mathcal{T}_1} \sum_{\boldsymbol{t_2} \in \mathcal{T}_2(\boldsymbol{t_1})} (-1)^{|\boldsymbol{t}|} \det(S(A : \boldsymbol{r_1}, \boldsymbol{t_1})) \det(S(A : \boldsymbol{r_2}, \boldsymbol{t_2})) \det(S'(A : \boldsymbol{r}, \boldsymbol{t})).$$

Note that the $\mathcal{T}_1$ and $\mathcal{T}_2$ are different from the ones in Example 1. Here, there are some zero blocks in A. In this case, $\mathcal{T}_1$ denotes the set of all 2-tuples $\boldsymbol{t_1} = (t_{1,1}, t_{1,2})$ for which $1 \leq t_{1,1} < t_{1,2} \leq 3$ and T_2 denotes the set of all 2-tuples $\boldsymbol{t_2} = (t_{2,1}, t_{2,2})$ for which $2 \leq t_{2,1} < t_{2,2} \leq 5$.

This example implies that Proposition 1 is more suitable for calculating the determinant function of the matrix which has more zero blocks in its submatrices consist of some columns.

3.2 The Second Class of Matrices

In this section, we introduce the calculation approach to the determinant function of another class of matrices with special form. These matrices will be applied to the construction of representable matroid associated to UCASs and LCASs. Recall that the determinant function is linear in the columns of a matrix as follows.

Proposition 2. *If a and b are scalars, $\bar{\boldsymbol{\alpha}}$ and $\bar{\boldsymbol{\beta}}$ are columns vectors, and B is some matrix, then* $\det\big((a\bar{\boldsymbol{\alpha}} + b\bar{\boldsymbol{\beta}}\ |B)\big) = a\det\big((\bar{\boldsymbol{\alpha}}\ |B)\big) + b\det\big((\bar{\boldsymbol{\beta}}\ |B)\big)$.

Example 3. Let $A_i = (a_{u,v})_{2\times 3}$ and $B_i = (b_{u,v})_{3\times 2}$ be a 2×3 matrix and a 3×2 matrix, respectively. Then $AB = \big(\sum_{i_1=1}^{3} b_{i_1,1}\bar{\boldsymbol{a}}_{\boldsymbol{i_1}} \big| \sum_{i_2=1}^{3} b_{i_2,2}\bar{\boldsymbol{a}}_{\boldsymbol{i_2}}\big)$ is a 2×2 matrix, where $\bar{\boldsymbol{a}}_{\boldsymbol{i}}$ denotes the ith column of A. Hence, from Proposition 2,

$$\begin{aligned}
\det(AB) &= \sum_{i_1=1}^{3} b_{i_1,1}\det\Big(\big(\bar{\boldsymbol{a}}_{\boldsymbol{i_1}}\big|\sum_{i_2=1}^{3} b_{i_2,2}\bar{\boldsymbol{a}}_{\boldsymbol{i_2}}\big)\Big)\\
&= \sum_{i_1=1}^{3}\sum_{i_2=1}^{3} b_{i_1,1}b_{i_2,2}\det\big((\bar{\boldsymbol{a}}_{\boldsymbol{i_1}}|\bar{\boldsymbol{a}}_{\boldsymbol{i_2}})\big)\\
&= b_{1,1}b_{2,2}\det\big((\bar{\boldsymbol{a}}_{\boldsymbol{1}}|\bar{\boldsymbol{a}}_{\boldsymbol{2}})\big) + b_{1,1}b_{3,2}\det\big((\bar{\boldsymbol{a}}_{\boldsymbol{1}}|\bar{\boldsymbol{a}}_{\boldsymbol{3}})\big) + b_{2,1}b_{1,2}\det\big((\bar{\boldsymbol{a}}_{\boldsymbol{2}}|\bar{\boldsymbol{a}}_{\boldsymbol{1}})\big)\\
&\quad + b_{2,1}b_{3,2}\det\big((\bar{\boldsymbol{a}}_{\boldsymbol{2}}|\bar{\boldsymbol{a}}_{\boldsymbol{3}})\big) + b_{3,1}b_{1,2}\det\big((\bar{\boldsymbol{a}}_{\boldsymbol{3}}|\bar{\boldsymbol{a}}_{\boldsymbol{1}})\big) + b_{3,1}b_{2,2}\det\big((\bar{\boldsymbol{a}}_{\boldsymbol{3}}|\bar{\boldsymbol{a}}_{\boldsymbol{2}})\big)\\
&= \sum_{1\le j_1<j_2\le 3}\det\begin{pmatrix} b_{j_1,1} & b_{j_1,2}\\ b_{j_2,1} & b_{j_2,2}\end{pmatrix}\det\big((\bar{\boldsymbol{a}}_{\boldsymbol{j_1}}|\bar{\boldsymbol{a}}_{\boldsymbol{j_2}})\big).
\end{aligned}$$

In general, we have the following proposition.

Proposition 3. *Take a $k\times k$ matrix $(AB|D)$ where $A = (a_{u,v})$ is a $k\times r$ matrix, $B = (b_{u,v})$ is a $r\times l$ matrix, and $k \ge r \ge l$, and take $\boldsymbol{j} = (j_1,\dots,j_l)$ such that $1 \le j_1 < \cdots < j_l \le r$. Let $A(\boldsymbol{j})$ and $B(\boldsymbol{j})$ denote the $k\times l$ submatrix formed by the j_1th column, …, j_lth column of A and the $l\times l$ submatrix formed by the j_1th row, …, j_lth row of B, respectively. Then*

$$\det\big((AB|D)\big) = \sum_{\boldsymbol{j}\in\mathcal{J}}\det\big(B(\boldsymbol{j})\big)\det\big((A(\boldsymbol{j})|D)\big),$$

where $\mathcal{J}$ denotes the set of all l-tuples $\boldsymbol{j} = (j_1,\dots,j_l)$ for which $1 \le j_1 < \cdots < j_l \le r$.

Proof. If there are two identical columns in a square matrix, then its determinant equals 0. Therefore, from this and Proposition 2,

$$\begin{aligned}
\det\big((AB|D)\big) &= \det\Big(\Big(\sum_{i_1=1}^{r} b_{i_1,1}\bar{\boldsymbol{a}}_{\boldsymbol{i_1}}\Big|\cdots\Big|\sum_{i_l=1}^{r} b_{i_l,l}\bar{\boldsymbol{a}}_{\boldsymbol{i_l}}\Big|\ D\Big)\Big)\\
&= \sum_{i_v\in[r],v\in[l]}\Big(\prod_{v\in[l]} b_{i_v,v}\Big)\det\big((\bar{\boldsymbol{a}}_{\boldsymbol{i_1}}|\cdots|\bar{\boldsymbol{a}}_{\boldsymbol{i_l}}|D)\big)\\
&= \sum_{\boldsymbol{i}}\Big(\prod_{v\in[l]} b_{i_v,v}\Big)\det\big((\bar{\boldsymbol{a}}_{\boldsymbol{i_1}}|\cdots|\bar{\boldsymbol{a}}_{\boldsymbol{i_l}}|D)\big),
\end{aligned}$$

where the summation is over all l-tuples $\boldsymbol{i} = (i_1, \ldots, i_l)$ for which $i_v \in [r]$ and $i_v \neq i_{v'}$, $v \neq v' \in [l]$.

For a given $\boldsymbol{j} = (j_1, \ldots, j_l)$ such that $1 \leq j_1 < \cdots < j_l \leq r$, let $S(\boldsymbol{j})$ denote the set of all the permutations on the set $\{j_1, \ldots, j_l\}$. we claim that

$$\sum_{\boldsymbol{i} \in S(\boldsymbol{j})} \Big(\prod_{v \in [l]} b_{i_v, v} \Big) \det \big((\bar{\boldsymbol{a}}_{\boldsymbol{i}_1} | \cdots | \bar{\boldsymbol{a}}_{\boldsymbol{i}_l} | D) \big) = \det \big(B(\boldsymbol{j}) \big) \det \big((A(\boldsymbol{j}) | D) \big)$$

Without loss of generality, we may assume that $\boldsymbol{j} = (1, \ldots, l)$, that is $j_v = v$ with $v \in [l]$. Then

$$\Big(\prod_{v \in [l]} b_{i_v, v} \Big) \det \big((\bar{\boldsymbol{a}}_{\boldsymbol{i}_1} | \cdots | \bar{\boldsymbol{a}}_{\boldsymbol{i}_l} | D) \big) = \operatorname{sgn}(\boldsymbol{i}) \Big(\prod_{v \in [l]} b_{i_v, v} \Big) \det \big((\bar{\boldsymbol{a}}_{\boldsymbol{1}} | \cdots | \bar{\boldsymbol{a}}_{\boldsymbol{l}} | D) \big),$$

where $\operatorname{sgn}(\boldsymbol{i})$ denotes the sign of $\boldsymbol{i}$. Note that for $\boldsymbol{j} = (1, \ldots, l)$,

$$\sum_{\boldsymbol{i} \in S(\boldsymbol{j})} \operatorname{sgn}(\boldsymbol{i}) \Big(\prod_{v \in [l]} b_{i_v, v} \Big) = \det \big(B(\boldsymbol{j}) \big).$$

This implies the claim, and the result follows. □

We next give a formula to calculate the determinant function of a matrix with special form which will be used to the scheme for UCASs and LCASs.

Proposition 4. *Let $G = (A_1 B_1 | \cdots | A_m B_m)$ be a $k \times k$ matrix such that A_i is a $k \times r_i$ block and B_i is a $r_i \times l_i$ block, where $l_i \leq r_i \leq k$ and $\sum_{i=1}^{m} l_i = k$. For any $\boldsymbol{j_i} = (j_{i,1}, \ldots, j_{i,l_i})$ with $i \in J_m$ such that $1 \leq j_{i,1} < \cdots < j_{i,l_i} \leq r_i$, let $A_i(\boldsymbol{j_i})$ and $B_i(\boldsymbol{j_i})$ denote the $k \times l_i$ submatrix formed by the $j_{i,1}$th column, ..., j_{i,l_i}th column of A_i and the $l_i \times l_i$ submatrix formed by the $j_{i,1}$th row, ..., j_{i,l_i}th row of B_i, respectively. Then*

$$\det(G) = \sum_{\boldsymbol{j}_i, i \in [m]} \Big(\prod_{i=1}^{m} \det \big(B_i(\boldsymbol{j_i}) \big) \Big) \det \Big(\big(A_1(\boldsymbol{j_1}) | \cdots | A_m(\boldsymbol{j_m}) \big) \Big),$$

where the summation is over all l_i-tuples $\boldsymbol{j_i} = (j_{i,1}, \ldots, j_{i,l_i})$ with $i \in J_m$, for which $1 \leq j_{i,1} < \cdots < j_{i,l_i} \leq r_i$.

Proof. Let $A_i := (a_{u,v}^{(i)})$ with $u \in [k]$ and $v \in [r_i]$, $B_i := (b_{u,v}^{(i)})$ with $u \in [r_i]$ and $v \in [l_i]$, and $\bar{\boldsymbol{a}}_j^{(\boldsymbol{i})}$ denote the jth column of matrix A_i. From Proposition 3,

$$\begin{aligned} \det(G) &= \det \Big(\Big(\sum_{i_{1,1}=1}^{r_1} b_{i_{1,1},1}^{(1)} \bar{\boldsymbol{a}}_{\boldsymbol{i_{1,1}}}^{(\boldsymbol{1})} \Big| \cdots \Big| \sum_{i_{1,l_1}=1}^{r_1} b_{i_{1,l_1},l_1}^{(1)} \bar{\boldsymbol{a}}_{\boldsymbol{i_{1,l_1}}}^{(\boldsymbol{1})} \Big| A_2 B_2 \Big| \cdots \Big| A_m B_m \Big) \Big) \\ &= \sum_{\boldsymbol{j_1}} \det \big(B_1(\boldsymbol{j_1}) \big) \det \Big(\big(A_1(\boldsymbol{j_1}) | A_2 B_2 | \cdots | A_m B_m \big) \Big), \end{aligned}$$

where the summation is over all l_1-tuples $\boldsymbol{j_1} = (j_{1,1}, \ldots, j_{1,l_1})$, for which $1 \leq j_{1,1} < \cdots < j_{1,l_1} \leq r_1$. The conclusion can be obtained by computing $A_i B_i$ for $i \in [2, m]$ using the similar method to $A_1 B_1$. □

4 Secret Sharing Schemes for Ideal Hierarchical Access Structures

In this section, we construct ideal linear secret sharing schemes realizing IHASs by an efficient method. We will present two classes of constructions based on the same representation of an integer polymatroid. We first present an integer polymatroid $\mathcal{Z}'$ satisfying Theorem 2 such that the IHASs (1) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$.

Given two vectors $\hat{\boldsymbol{k}}, \boldsymbol{k} \in \mathbb{Z}_+^{J'_m}$ such that $\hat{k}_0 = \hat{k}_1 = 0$, $k_0 = 1$, $k_m = k$, and $\hat{k}_i \le \hat{k}_{i+1} < k_i \le k_{i+1}$ for $i \in [0, m-1]$, consider the subsets $S_i = [\hat{k}_i + 1, k_i]$ of the set $S = [k]$ and the Boolean polymatroid $\mathcal{Z}' = \mathcal{Z}'(\hat{\boldsymbol{k}}, \boldsymbol{k})$ with ground J'_m defined from them. The following result was presented in Section IX of [18].

Lemma 1. *Let $\Pi = (\Pi_i)_{i \in J_m}$ be a partition of the set P with $|\Pi_i| \ge h(\{i\}) = k_i - \hat{k}_i$. Then the IHASs (1) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$.*

Now we introduce a linear representation of the polymatroid defined in Lemma 1, that is a collection $(V_i)_{i \in J'_m}$ of subspaces of some vector space. Recalled that Boolean polymatroids are representable over every finite field. Here, we give a simple representation of $\mathcal{Z}'$ based on the unit matrix as follows.

Take a $k \times k$ unit matrix I_k, and for every $i \in J'_m$, let E_i denote the submatrix formed by the $(\hat{k}_i+1)$th column to the k_ith column of I_k. Consider the $\mathbb{F}_q$-vector subspace $V_i \subseteq \mathbb{F}_q^k$ spanned by all the columns of E_i. Let the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ such that $h(X) = \dim\left(\sum_{i \in X} V_i\right)$ for every $X \subseteq J'_m$. We have the following result.

Proposition 5. *For the integer polymatroid $\mathcal{Z}'$ defined above, the IHASs (1) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$ and $\mathcal{B}(\mathcal{Z}') = \mathcal{B}_1 \cup \mathcal{B}_2$, where*

$$\mathcal{B}_1 = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = k, u_0 = 0 \text{ and } \hat{k}_{i+1} \le |\boldsymbol{u}([i])| \le k_i \text{ for all } i \in [m-1]\}, \tag{6}$$

$$\mathcal{B}_2 = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = k, u_0 = 1 \text{ and } \hat{k}_{i+1} - 1 \le |\boldsymbol{u}([i])| \le k_i - 1 \text{ for all } i \in [m-1]\}.$$

Proof. Suppose the set $S = [k]$ and the subsets $S_i = [\hat{k}_i + 1, k_i]$ for every $i \in J'_m$. Then for every $X \subseteq J'_m$, $h(X) = \dim\left(\sum_{i \in X} V_i\right) = |\cup_{i \in X} S_i|$. This implies $\mathcal{Z}'$ is a linear representation of the polymatroid $\mathcal{Z}'(\hat{\boldsymbol{k}}, \boldsymbol{k})$, and the first claim follows. In addition, since I_k is nonsingular and E_i is an submatrix of I_k for every $i \in J'_m$, it follows that any k distinct columns vectors from E_i with $i \in J'_m$ are linearly independent, and the second claim follows. □

This proposition implies that the collection $(V_i)_{i \in J'_m}$ is a linear representation of the integer polymatroid $\mathcal{Z}'$ associated to the IHASs (1). We will present two class of constructions for ideal linear schemes realizing IHASs by representable matroids obtained based on $\mathcal{Z}'$.

4.1 Construction for Ideal Hierarchical Access Structures

In this section, we represent a class of ideal linear scheme for IHASs, which can be obtained by a representation of the matroid associated to IHASs.

Suppose $\Pi_0 = \{p_0\}$ and let $\Pi' = (\Pi_i)_{i\in J'_m}$ and $\Pi = (\Pi_i)_{i\in J_m}$ be the partition of $P' = P \cup \{p_0\}$ and P, respectively, such that $|\Pi_i| = n_i$. For every $i \in J_m$, take different elements $\beta_{i,v} \in \mathbb{F}\backslash\{0\}$ with $v \in [n_i]$ and define a $(k_i - \hat{k}_i) \times n_i$ matrix

$$B_i = \left((\beta_{i,v}x^{m-i})^{u-1}\right) \qquad u \in [k_i - \hat{k}_i],\ v \in [n_i].$$

Let a $k \times (n+1)$ matrix be defined as

$$M = (M_0|M_1|\cdots|M_m), \tag{7}$$

where $M_0 = (1, 0, \ldots, 0)^T$ is a k-dimensional column vector and $M_i = E_iB_i$ for every $i \in J_m$. Then the secret sharing scheme $LSSS(M)$ is as follows:

Secret Sharing Scheme.

1. Let $s \in \mathbb{K}$ be a secret value. The dealer chooses randomly a k-dimensional vector $\boldsymbol{a}$ such that $\boldsymbol{a}M_0 = s$;
2. The share of each participant $p_{i,j}$ from compartment Π_i is $\boldsymbol{a}\boldsymbol{b}_{\boldsymbol{i,j}}^{\boldsymbol{T}}$, where $\boldsymbol{b}_{\boldsymbol{i,j}}^{\boldsymbol{T}}$ denotes the jth column of M_i with $i \in J_m$ and $j \in [n_i]$.

We proceed to show that $LSSS(M)$ is a perfect ideal linear scheme realizing IHASs. This can be done by proving M is a representation of the matroid associated the IHASs (1). Obviously, M satisfies the first two conditions in Step 3 of Sect. 2.3. We will prove that it satisfies the third condition too. We first give the following lemmas.

Lemma 2. *For any $\boldsymbol{u} \in \mathcal{B}_1$, (6), $\det(M_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree at most K where*

$$K = \frac{1}{2}\sum_{i=1}^{m-1} k_i(k_i - 1) - \sum_{i=2}^{m-1}(m-i)(k_i - k_{i-1})\hat{k}_i.$$

Proof. For every $i \in J_m$, take

$$B'_i = \left(\beta_{i,v}^{u-1}\right) \quad u \in [k_i - \hat{k}_i],\ v \in [n_i],$$

and for any $\boldsymbol{u} \in \mathcal{B}_1$, (6), let $B_i(u_i)$ and $B'_i(u_i)$ denote the submatrices formed by any u_i columns in B_i and B'_i, respectively.

Let us exemplify how such an event may occur. Assume, for example, that $m = 3$, $\boldsymbol{k} = (k_1, k_2, k_3) = (3, 5, 7)$, $\hat{\boldsymbol{k}} = (\hat{k}_1, \hat{k}_2, \hat{k}_3) = (0, 1, 2)$. Take $\boldsymbol{u} = (u_1, u_2, u_3) = (2, 2, 3)$ and the corresponding matrix $M_{\boldsymbol{u}}$ has the following form:

$$M_{\boldsymbol{u}} = \left(\begin{array}{cc|cc|ccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ \beta_{1,1}x^2 & \beta_{1,2}x^2 & 1 & 1 & 0 & 0 & 0 \\ (\beta_{1,1}x^2)^2 & (\beta_{1,2}x^2)^2 & \beta_{2,1}x & \beta_{2,2}x & 1 & 1 & 1 \\ 0 & 0 & (\beta_{2,1}x)^2 & (\beta_{2,2}x)^2 & \beta_{3,1} & \beta_{3,2} & \beta_{3,3} \\ 0 & 0 & (\beta_{2,1}x)^3 & (\beta_{2,2}x)^3 & \beta_{3,1}^2 & \beta_{3,2}^2 & \beta_{3,3}^2 \\ 0 & 0 & 0 & 0 & \beta_{3,1}^3 & \beta_{3,2}^3 & \beta_{3,3}^3 \\ 0 & 0 & 0 & 0 & \beta_{3,1}^4 & \beta_{3,2}^4 & \beta_{3,3}^4 \end{array}\right).$$

Suppose $1 \le t_{1,1} < t_{1,2} \le 3$, $2 \le t_{2,1} < t_{2,2} \le 5$, $3 \le t_{3,1} < t_{3,2} < t_{3,3} \le 7$, and $\{t_{1,1}, t_{1,2}, t_{2,1}, t_{2,2}, t_{3,1}, t_{3,2}, t_{3,3}\} = [7]$. Let $\hat{B}_1$ and $\hat{B}'_1$ be the blocks formed by the $t_{1,1}$th and $t_{1,2}$th rows of $B_1(u_1)$ and $B'_1(u_1)$, respectively, $\hat{B}_2$ and $\hat{B}'_2$ be the blocks formed by the $t_{2,1}$th and $t_{2,2}$th rows of $B_2(u_2)$ and $B'_2(u_2)$, respectively, and $\hat{B}_3$ and $\hat{B}'_3$ be the blocks formed by the $t_{3,1}$th, $t_{3,2}$th and $t_{3,3}$th rows of $B_3(u_3)$ and $B'_3(u_3)$, respectively. Then Proposition 1 implies that the summation in $\det(M_{\boldsymbol{u}})$ can be denoted by

$$|a_t x^t| := \det(\hat{B}_1)\det(\hat{B}_2)\det(\hat{B}_3) = \det(\hat{B}'_1)\det(\hat{B}'_2)\det(\hat{B}'_3)x^t$$

where $t = 2(t_{1,1}-1)+2(t_{1,2}-1)+(t_{2,1}-2)+(t_{2,2}-2)$. Therefore, when $t_{1,1}=1$, $t_{1,2}=2$, $t_{2,1}=3$ and $t_{2,2}=4$, t is minimal. In this case $t=5$ and $\hat{B}'_i$ with $i \in [3]$ are all nonsingular. This implies $a_5 \neq 0$.

In addition, take $\boldsymbol{u'} = (u'_1, u'_2, u'_3)$ such that $\boldsymbol{u'}([i]) = k_i$ for every $i \in [3]$. Then $\boldsymbol{u'} \in \mathcal{B}_1$. In this case let $t'_{1,1}=1$, $t'_{1,2}=2$, $t'_{1,3}=3$, $t'_{2,1}=4$, $t'_{2,2}=5$, $t'_{3,1}=6$ and $t'_{3,2}=7$, then $t \le 2\sum_{i'=1}^{3}(t'_{1,i'}-1)+\sum_{i'=1}^{2}(t'_{2,i'}-2) = 11$. Therefore, $\det(M_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree at most 11. In fact, by computing, we have $t < 11$.

In general, for any $\boldsymbol{u} \in \mathcal{B}_1$, let $\hat{B}_i$ and $\hat{B}'_i$ be the blocks formed by all the $t_{i,i'}$th rows of $B_i(u_i)$ and $B'_i(u_i)$, respectively, where $i' \in [u_i]$ such that

$$\hat{k}_i + 1 \le t_{i,1} < \cdots < t_{i,u_i} \le k_i \text{ and } \bigcup\nolimits_{i=1}^{m} \{t_{i,i'} : i' \in [u_i]\} = [k].$$

Then Proposition 1 implies that the summation in $\det(M_{\boldsymbol{u}})$ can be denoted by

$$|a_t x^t| = \prod\nolimits_{i=1}^{m} \det(\hat{B}_i) = \prod\nolimits_{i=1}^{m} \det(\hat{B}'_i)x^t$$

where

$$t = \sum_{i=1}^{m-1}\Big((m-i)\sum_{i'=1}^{u_i}(t_{i,i'}-\hat{k}_i-1)\Big) = \sum_{j=1}^{m-1}\Big(\sum_{i=1}^{j}\Big(\sum_{i'=1}^{u_i}(t_{i,i'}-\hat{k}_i-1)\Big)\Big). \quad (8)$$

For every $j \in [m-1]$, take $T_j = \sum_{i=1}^{j}\big(\sum_{i'=1}^{u_i}(t_{i,i'}-\hat{k}_i-1)\big)$. We have that T_{m-1} is minimal if $\bigcup_{i=1}^{m-1}\{t_{i,i'} : i' \in [u_i]\} = \big[|\boldsymbol{u}([m-1])|\big]$. In this case T_{m-2} is minimal if $\bigcup_{i=1}^{m-2}\{t_{i,i'} : i' \in [u_i]\} = \big[|\boldsymbol{u}([m-2])|\big]$. Therefore, t is minimal if $\bigcup_{i=1}^{j}\{t_{i,i'} : i' \in [u_i]\} = \big[|\boldsymbol{u}([j])|\big]$ for all $j \in [m-1]$. This implies that $t_{1,i'} = i'$ and $t_{i,i'} = |\boldsymbol{u}([i-1])| + i'$ for $i \in [2, m-1]$. Hence,

$$t \ge (m-1)\sum_{i'=1}^{u_1}(i'-1) + \sum_{i=2}^{m-1}\Big((m-i)\sum_{i'=1}^{u_i}\big(|\boldsymbol{u}([i-1])| + i' - \hat{k}_i - 1\big)\Big) = t_0.$$

In this case each $\hat{B}'_i$ is nonsingular since it is the square submatrix formed by the successive u_i rows of $B'_i(u_i)$. This implies that $a_{t_0} \neq 0$.

In addition, take a vector $\boldsymbol{u'} \in \mathbb{Z}_+^m$ such that $|\boldsymbol{u}([i])| = k_i$ for every $i \in J_m$. Then $\boldsymbol{u'} \in \mathcal{B}_1$. In this case $t_{1,i'} = i'$ with $i' \in [k_1]$ and $t'_{i,i'} = k_{i-1} + i'$ with $i \in [2, m-1]$ and $i' \in [k_i - k_{i-1}]$. Then

$$\begin{aligned} t &\le (m-1)\sum_{i'=1}^{k_1}(i'-1) + \sum_{i=2}^{m-1}\Big((m-i)\sum_{i'=1}^{k_i-k_{i-1}}(k_{i-1}+i'-\hat{k}_i-1)\Big) \\ &= (m-1)\sum_{i'=1}^{k_1}(i'-1) + \sum_{i=2}^{m-1}\Big((m-i)\sum_{i'=1}^{k_i-k_{i-1}}(k_{i-1}+i'-1)\Big) - \sum_{i=2}^{m-1}(m-i)\sum_{i'=1}^{k_i-k_{i-1}}\hat{k}_i \\ &= \sum_{i=1}^{m-1}(1+2+\cdots+(k_i-1)) - \sum_{i=2}^{m-1}(m-i)(k_i-k_{i-1})\hat{k}_i \\ &= \frac{1}{2}\sum_{i=1}^{m-1}k_i(k_i-1) - \sum_{i=2}^{m-1}(m-i)(k_i-k_{i-1})\hat{k}_i. \end{aligned} \tag{9}$$

This implies the conclusion.

Lemma 3. *For any $\boldsymbol{u} \in \mathcal{B}_2$, (6), $\det(M_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree at most K.*

Proof. Let M' denote the submatrix obtained by removing the first row and the first column of M and take $\boldsymbol{k'}, \hat{\boldsymbol{k}}' \in \mathbb{Z}_+^m$ such that for every $i \in J_m$, $k'_i = k_i - 1$, and $\hat{k}'_i = \hat{k}_i$ if $\hat{k}_i = 0$ and $\hat{k}'_i = \hat{k}_i - 1$ if $\hat{k}_i > 0$. For every $i \in J_m$, let E'_i denote the submatrix formed by the $(\hat{k}'_i + 1)$th column to the k'_ith column of I_{k-1}. Let D_1 and D'_1 denote the submatrices formed by the last k'_1 rows of B_1 and B'_1, respectively. For every $i \in [2, m]$, if $\hat{k}_i = 0$, let D_i and D'_i denote the submatrices formed by the last $k'_i - 1$ rows of B_i and B'_i, respectively, and if $\hat{k}_i > 0$, let $D_i = B_i$ and $D'_i = B'_i$. Then

$$M' = (M'_1|\cdots|M'_m)$$

where $M'_i = E'_i D_i$ and for any $\boldsymbol{u} \in \mathcal{B}_2$, (6), $\det(M_{\boldsymbol{u}}) = \det\left(M'_{\boldsymbol{u}(J_m)}\right)$. In particular, for any $\boldsymbol{u} \in \mathcal{B}_2$, (6), $\hat{k}'_{i+1} \le |\boldsymbol{u}([i])| \le k'_i$ for all $i \in [m-1]$ and $|\boldsymbol{u}| = k-1$. Therefore, this claim can be proved by the same method in the proof of Lemma 2.

For any $\boldsymbol{u} \in \mathcal{B}_2$, (6), let $D'_i(u_i)$ denote the block formed by any u_i columns in D'_i, and let $\hat{D}'_i$ be the block formed by all the $t_{i,i'}$th rows of $D'_i(u_i)$. Here, $i' \in [u_i]$ such that $\hat{k}'_i + 1 \le t_{i,1} < \cdots < t_{i,u_i} \le k'_i$ and $\bigcup_{i=1}^m \{t_{i,i'} : i' \in [u_i]\} = [k-1]$. Then the summation in $\det\left(M'_{\boldsymbol{u}(J_m)}\right)$ can be denoted by $|b_{t'}x^{t'}| = \prod_{i=1}^m \det(\hat{D}'_i)x^{t'}$. Similar to (8),

$$t' = \sum_{i=1}^{m-1}\Big((m-i)\sum_{i'=1}^{u_i}(t_{i,i'} - \hat{k}'_i - y_i)\Big)$$

where $y_i = 0$ if $\hat{k}'_i = 0$ and $y_i = 1$ if $\hat{k}'_i > 0$. From $\hat{k}'_i = \hat{k}_i$ if $\hat{k}_i = 0$ and $\hat{k}'_i = \hat{k}_i - 1$ if $\hat{k}_i > 0$, we have

$$t' = \sum_{i=1}^{m-1}\Big((m-i)\sum_{i'=1}^{u_i}(t_{i,i'} - \hat{k}_i)\Big).$$

Similar to the proof in Lemma 2, we can obtain t' is minimal if $t_{1,i'} = i'$ and $t_{i,i'} = |\boldsymbol{u}([i-1])| + i'$ for $i \in [2, m-1]$, and in this case each $\hat{D}'_i$ is nonsingular, thus $\det\left(M'_{\boldsymbol{u}(J_m)}\right)$ is a nonzero polynomial on x. In addition, take a vector $\boldsymbol{u'} \in \mathbb{Z}_+^m$ such that $|\boldsymbol{u}([i])| = k'_i$ for every $i \in J_m$. Then $\hat{k}'_{i+1} \leq |\boldsymbol{u'}([i])| \leq k'_i$ for all $i \in [m-1]$ and $|\boldsymbol{u'}| = k-1$. In this case $t_{1,i'} = i'$ with $i' \in [k'_1]$ and $t'_{i,i'} = k'_{i-1} + i'$ with $i \in [2, m-1]$ and $i' \in [k'_i - k'_{i-1}]$. Similar to (9),

$$\begin{aligned} t' &\leq (m-1)\sum_{i'=1}^{k'_1} i' + \sum_{i=2}^{m-1}\left((m-i)\sum_{i'=1}^{k'_i-k'_{i-1}}(k'_{i-1}+i'-\hat{k}_i)\right) \\ &= (m-1)\sum_{i'=1}^{k_1}(i'-1) + \sum_{i=2}^{m-1}\left((m-i)\sum_{i'=1}^{k_i-k_{i-1}}(k_{i-1}+i'-\hat{k}_i-1)\right) = K \end{aligned}$$

since $k'_i = k_i - 1$ for every $i \in J_m$. This implies $\det\left(M'_{\boldsymbol{u}(J_m)}\right)$ is a nonzero polynomial on x of degree at most K, and the claim follows. □

The following result was proved by Shoup [33].

Theorem 4 ([33])**.** *Take a finite field $\mathbb{F}_{q^\lambda}$ where q is a prime power and λ is a positive integer. Then there exists an element $x \in \mathbb{F}_{q^\lambda}$ such that its minimal polynomial over $\mathbb{F}_q$ is of degree λ which can be found in time $O(q, \lambda)$.*

Now, take a finite field $\mathbb{F}_{q^\lambda}$, where $q > \max_{i\in J_m}\{n_i\}$ is a prime power and $\lambda > K$. Take all $\beta_{i,v}$ in the matrix (7) from $\mathbb{F}_q \backslash \{0\}$ and take $x \in \mathbb{F}_{q^\lambda}$ such that its minimal polynomial over $\mathbb{F}_q$ is of degree λ. We have the following result.

Theorem 5. *The matrix (7) is a representation of the matroid associated to IHASs (1) over $\mathbb{F}_{q^\lambda}$ for some prime power $q > \max_{i\in J_m}\{n_i\}$ and some $\lambda > K$. Moreover, such a representation can be obtained in time $O(q, \lambda)$.*

Proof. Since all the entries in the matrix (7), except the powers of x, are in $\mathbb{F}_q$, and Theorem 4 implies that such an element x can be found in time $O(q, \lambda)$, it follows that for any $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, (6), $\det(M_{\boldsymbol{u}})$ must be a nonzero $\mathbb{F}_q$-polynomial on x with degree smaller than λ, and consequently, the matrix $M_{\boldsymbol{u}}$ is nonsingular. This implies the claim. □

Proposition 6. *Suppose M is the matrix (7). Then $LSSS(M)$ realizes the IHASs (1) over $\mathbb{F}_{q^\lambda}$ defined as in Theorem 5. Moreover, such a scheme can be obtained in time $O(q, \lambda)$.*

Proof. Theorem 1 implies that proving this claim is equivalent to proving that $\boldsymbol{v}(J_m) \in \Gamma$ if and only M_0 is a linear combination of all the columns in $M_{\boldsymbol{v}(J_m)}$.

Let $\boldsymbol{v}(J_m) \in \min \Gamma$, (1), namely, $\boldsymbol{v}(J_m) = (v_1, v_2, \ldots, v_\ell, 0, \ldots, 0)$ for some $\ell \in J_m$ such that $\hat{k}_{i+1} \leq |\boldsymbol{v}([i])| < k_i$ for all $i \in [\ell - 1]$ and $|\boldsymbol{v}([\ell])| = k_\ell$. Then there must exist a vector $\boldsymbol{u} \in \mathcal{B}_1$, (6), such that $\boldsymbol{u} \geq \boldsymbol{v}$ and $u_i = v_i$ for every

$i \in [\ell]$. Note that the last $k-k_\ell$ rows of $M_{\boldsymbol{v}(J_m)}$ are all zero rows, it follows that $M_{\boldsymbol{u}(J_m)}$ has the following form

$$M_{\boldsymbol{u}(J_m)} = \begin{pmatrix} \hat{M}_{\boldsymbol{v}(J_m)} & A_1 \\ O & A_2 \end{pmatrix}$$

where $\hat{M}_{\boldsymbol{v}(J_m)}$ is the square block formed by the first k_ℓ rows of $M_{\boldsymbol{v}(J_m)}$, A_1 is a $(k-k_\ell)\times k_\ell$ block and A_2 is a $(k-k_\ell)\times(k-k_\ell)$ block. From Theorem 5, $M_{\boldsymbol{u}(J_m)}$ is nonsingular. This with $\det(M_{\boldsymbol{u}(J_m)}) = \det(\hat{M}_{\boldsymbol{v}(J_m)})\cdot\det(A_2)$ implies that $\hat{M}_{\boldsymbol{v}(J_m)}$ is nonsingular. In this case, the k_ℓ-dimensional column vector formed by the first k_ℓ elements of M_0 can be spanned by the columns of $\hat{M}_{\boldsymbol{v}(J_m)}$. Accordingly, M_0 can be spanned by the columns in $M_{\boldsymbol{v}(J_m)}$ as the last $k-k_\ell$ elements of M_0 are all zero. Hence, M_0 can be spanned by the columns in $M_{\boldsymbol{v}(J_m)}$ for any $\boldsymbol{v}(J_m) \in \Gamma$.

Assume that $\boldsymbol{v}(J_m) \notin \Gamma$. We know every unauthorized subset may be completed into an authorized subset (though not necessarily minimal) by adding to it at most k participants. Without loss of generality, we may assume that there exists a vector $\boldsymbol{v'}(J_m) \in \Gamma$ such that $\boldsymbol{v'}(J_m) \geq \boldsymbol{v}(J_m)$ and $|\boldsymbol{v'}(J_m)| = |\boldsymbol{v}(J_m)|+1$.

First, assume that $\boldsymbol{v}(J_m) = (v_1, v_2, \ldots, v_\ell, 0, \ldots, 0)$ for some $\ell \in J_m$ such that $\hat{k}_{i+1} - 1 \leq |\boldsymbol{v}([i])| \leq k_i - 1$ for all $i \in [\ell-1]$ and $|\boldsymbol{v}([\ell])| = k_\ell - 1$. Then for the vector $\boldsymbol{v}(J'_m)$ with $u_0 = 1$, namely, $\boldsymbol{v}(J'_m) = (1, v_1, v_2, \ldots, v_\ell, 0, \ldots, 0)$, there must exist a vector $\boldsymbol{u}(J'_m) \in \mathcal{B}_2$, (6), such that $\boldsymbol{u}(J'_m) \geq \boldsymbol{v}(J'_m)$ and $u_i = v_i$ for every $i \in [0, \ell]$. From Theorem 5, $M_{\boldsymbol{u}(J'_m)}$ is nonsingular. This with $\boldsymbol{v}(J_m) \leq \boldsymbol{u}(J_m)$ implies that M_0 can't be spanned by all the columns in $M_{\boldsymbol{v}(J_m)}$.

Second, assume that $\boldsymbol{v}(J_m) = (v_1, v_2, \ldots, v_m)$ with $|\boldsymbol{v}(J_m)| \geq k$ such that for some $\ell \in J_m$, $|\boldsymbol{v}([\ell])| = \hat{k}_{l+1} - 1$, $\hat{k}_{i+1} - 1 \leq |\boldsymbol{v}([i])| < k_i$ for every $i \in [\ell-1]$, and $v_i = n_i$ for every $i \in [\ell+1, m]$. Then M_0 can't be spanned by the columns in $M_{\boldsymbol{v'}(J_m)}$ for any $\boldsymbol{v'}(J_m) \leq \boldsymbol{v}(J_m)$ if M_0 can't be spanned by the columns in $M_{\boldsymbol{v}(J_m)}$. We claim that every column in $M_{\boldsymbol{v}(J_m)}$ can be spanned by the columns in $M_{\boldsymbol{u}(J_m)}$ for any $\boldsymbol{u}(J_m) \leq \boldsymbol{v}(J_m)$ with $|\boldsymbol{u}(J_m)| = k-1$ such that $|\boldsymbol{u}([i])| = |\boldsymbol{v}([i])|$ for every $i \in [l]$ and $\hat{k}_{i+1} - 1 \leq |\boldsymbol{u}([i])| < k_i$ for every $i \in [\ell+1, m-1]$.

For such a vector $\boldsymbol{u}(J_m)$, if $u_0 = 1$, then $\boldsymbol{u}(J'_m) \in \mathcal{B}_2$, (6). This implies M_0 can't be spanned by the columns in $M_{\boldsymbol{u}(J_m)}$. Furthermore, M_0 can't be spanned by the columns in $M_{\boldsymbol{v}(J_m)}$ if the claim is true.

We proceed to prove the claim. Note that

$$M_{\boldsymbol{u}(J'_m)} = \left(M_{\boldsymbol{u}([0,\ell])} \middle| M_{\boldsymbol{u}([\ell+1,m])} \right) = \begin{pmatrix} D_1 & O \\ D_2 & \bar{M}_{\boldsymbol{u}([\ell+1,m])} \end{pmatrix}$$

where $\bar{M}_{\boldsymbol{u}([\ell+1,m])}$ is the square block formed by the last $k - \hat{k}_{\ell+1}$ rows of $M_{\boldsymbol{u}([\ell+1,m])}$. As $M_{\boldsymbol{u}(J'_m)}$ is nonsingular, thus $\bar{M}_{\boldsymbol{u}([\ell+1,m])}$ is nonsingular. On the other hand, $M_{\boldsymbol{v}(J_m)} = \left(M_{\boldsymbol{v}([\ell])} \middle| M_{\boldsymbol{v}([\ell+1,m])} \right)$, where

$$M_{\boldsymbol{v}([\ell+1,m])} = \begin{pmatrix} O \\ \bar{M}_{\boldsymbol{v}([\ell+1,m])} \end{pmatrix}$$

for which $\bar{M}_{\boldsymbol{v}([\ell+1,m])}$ is the block formed by the last $k-\hat{k}_{\ell+1}$ rows of $M_{\boldsymbol{v}([\ell+1,m])}$. Since $\bar{M}_{\boldsymbol{u}([\ell+1,m])}$ is a submatrix of $\bar{M}_{\boldsymbol{v}([\ell+1,m])}$ and $\bar{M}_{\boldsymbol{u}([\ell+1,m])}$ is nonsingular,

it follows that any column in $\bar{M}_{\boldsymbol{v}([\ell+1,m])}$ can be spanned by the columns in $\bar{M}_{\boldsymbol{u}([\ell+1,m])}$. Accordingly, any column in $M_{\boldsymbol{v}([\ell+1,m])}$ is a linear combination of the columns in $M_{\boldsymbol{u}([\ell+1,m])}$. This with $M_{\boldsymbol{v}([\ell])} = M_{\boldsymbol{u}([\ell])}$ implies the claim. □

4.2 Another Construction for Ideal Hierarchical Access Structures

In this section, we give another construction of ideal linear secret sharing schemes for IHASs using the similar technique in Sect. 4.1. The parameters of this construction may be better than the construction in Sect. 4.1 in some cases.

For every $i \in J_m$, take n_i different elements $\beta_{i,v} \in \mathbb{F}\backslash\{0\}$ and let the $(k_i - \hat{k}_i) \times n_i$ matrix B_i be defined as follows:

$$B_i = \left((\beta_{i,v}x^{i-1})^{k_i-\hat{k}_i-u}\right) \quad u \in [k_i - \hat{k}_i],\ v \in [n_i].$$

Take a k-dimensional column vector $M_0 = (1, 0, \ldots, 0)^T$ and $M_i = E_iB_i$ for every $i \in J_m$. Define a $k \times (n+1)$ matrix as

$$M = (M_0|M_1|\cdots|M_m). \tag{10}$$

Similar to the case in Sect. 4.1, we will prove that $LSSS(M)$ realizes IHASs. First, we give an example to explain this construction as follows.

Example 4. As in Lemma 2, assume that $m = 3$, $\boldsymbol{k} = (k_1, k_2, k_3) = (3, 5, 7)$, and $\hat{\boldsymbol{k}} = (\hat{k}_1, \hat{k}_2, \hat{k}_3) = (0, 1, 2)$. Take $\boldsymbol{u} = (u_1, u_2, u_3) = (2, 2, 3)$ and the matrix $M_{\boldsymbol{u}}$ has the following form:

$$M_{\boldsymbol{u}} = \left(\begin{array}{cc|cc|ccc} \beta_{1,1}^2 & \beta_{1,2}^2 & 0 & 0 & 0 & 0 & 0 \\ \beta_{1,1} & \beta_{1,2} & (\beta_{2,1}x)^3 & (\beta_{2,2}x)^3 & 0 & 0 & 0 \\ 1 & 1 & (\beta_{2,1}x)^2 & (\beta_{2,2}x)^2 & (\beta_{3,1}x^2)^4 & (\beta_{3,2}x^2)^4 & (\beta_{3,3}x^2)^4 \\ 0 & 0 & \beta_{2,1}x & \beta_{2,2}x & (\beta_{3,1}x^2)^3 & (\beta_{3,2}x^2)^3 & (\beta_{3,3}x^2)^3 \\ 0 & 0 & 1 & 1 & (\beta_{3,1}x^2)^2 & (\beta_{3,2}x^2)^2 & (\beta_{3,3}x^2)^2 \\ 0 & 0 & 0 & 0 & \beta_{3,1}x^2 & \beta_{3,2}x^2 & \beta_{3,3}x^2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right).$$

Note that $M_{\boldsymbol{u}}$ can be transformed to the following form by exchanging rows and columns

$$\tilde{M}_{\boldsymbol{u}} = \left(\begin{array}{ccc|cc|cc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ \beta_{3,1}x^2 & \beta_{3,2}x^2 & \beta_{3,3}x^2 & 0 & 0 & 0 & 0 \\ (\beta_{3,1}x^2)^2 & (\beta_{3,2}x^2)^2 & (\beta_{3,3}x^2)^2 & 1 & 1 & 0 & 0 \\ (\beta_{3,1}x^2)^3 & (\beta_{3,2}x^2)^3 & (\beta_{3,3}x^2)^3 & \beta_{2,1}x & \beta_{2,2}x & 0 & 0 \\ (\beta_{3,1}x^2)^4 & (\beta_{3,2}x^2)^4 & (\beta_{3,3}x^2)^4 & (\beta_{2,1}x)^2 & (\beta_{2,2}x)^2 & 1 & 1 \\ 0 & 0 & 0 & (\beta_{2,1}x)^3 & (\beta_{2,2}x)^3 & \beta_{1,1} & \beta_{1,2} \\ 0 & 0 & 0 & 0 & 0 & \beta_{1,1}^2 & \beta_{1,2}^2 \end{array}\right),$$

Therefore, $|\det(M_{\boldsymbol{u}})| = |\det(\tilde{M}_{\boldsymbol{u}})|$.

Take $\boldsymbol{\kappa} = (\kappa_1, \kappa_2, \kappa_3) = (k - \hat{k}_3, k - \hat{k}_2, k - \hat{k}_1) = (5, 6, 7)$, and $\hat{\boldsymbol{\kappa}} = (\hat{\kappa}_1, \hat{\kappa}_2, \hat{\kappa}_3) = (k - k_3, k - k_2, k - k_1) = (0, 2, 4)$. Then Lemma 2 implies that $\det(\tilde{M}_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree at most L with

$$L = \frac{1}{2}\sum_{i=1}^{2} \kappa_i(\kappa_i - 1) - (\kappa_2 - \kappa_1)\hat{\kappa}_2 = 23.$$

Accordingly, $\det(M_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree at most L.

In general, we have the following lemma.

Lemma 4. *For any $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, (6), $\det(M_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree at most L where*

$$L = \frac{1}{2}\sum_{i=2}^{m}(k - \hat{k}_i)(k - \hat{k}_i - 1) - \sum_{i=2}^{m-1}(i-1)(\hat{k}_{i+1} - \hat{k}_i)(k - k_i).$$

Proof. For every $i \in J_m$, take

$$\tilde{B}_i = \left((\beta_{m-i+1,v}x^{m-i})^{u-1}\right) \qquad u \in [k_{m-i+1} - \hat{k}_{m-i+1}],\ v \in [n_{m-i+1}]$$

and let $\tilde{E}_i$ be the submatrix formed by the $(k - k_{m-i+1} + 1)$th column to the $(k - \hat{k}_{m-i+1})$th column of I_k. Let

$$\tilde{M} = (\tilde{M}_0|\tilde{M}_2|\cdots|\tilde{M}_m),$$

where $\tilde{M}_0 = (0, 0, \ldots, 0, 1)^T$ is a k-dimensional column vector and $\tilde{M}_i = \tilde{E}_i\tilde{B}_i$ for every $i \in J_m$. Take $\tilde{\Pi}_0 = \Pi_0$ and $\tilde{\Pi}_i = \Pi_{m-i+1}$ for every $i \in J_m$. Then $\tilde{\Pi} = (\tilde{\Pi}_i)_{i \in J'_m}$ is a partition of $P' = P \cup \{p_0\}$ too. Moreover, take $\boldsymbol{\kappa}, \hat{\boldsymbol{\kappa}} \in \mathbb{Z}_+^{J'_m}$ such that $\kappa_0 = k$, $\hat{\kappa}_0 = k - 1$, and for every $i \in J_m$, $\kappa_i = k - \hat{k}_{m-i+1}$ and $\hat{\kappa}_i = k - k_{m-i+1}$. Then $\hat{\kappa}_i \le \hat{\kappa}_{i+1} < \kappa_i \le \kappa_{i+1}$ for $i \in [m-1]$.

If $\boldsymbol{u} \in \mathcal{B}_1$, (6), then for any matrix $M_{\boldsymbol{u}}$, as in Example 4, by exchanging rows and columns we can obtain the matrix $\tilde{M}_{\boldsymbol{u}}$ such that $|\det(M_{\boldsymbol{u}})| = |\det(\tilde{M}_{\boldsymbol{u}})|$. As $\hat{k}_{m-i+1} \le |\boldsymbol{u}([m-i])| \le k_{m-i}$ for every $i \in [m-1]$,

$$\hat{\kappa}_{i+1} = k - k_{m-i} \le |\boldsymbol{u}([m-i+1, m])| \le k - \hat{k}_{m-i+1} = \kappa_i$$

for every $i \in [m-1]$. From Lemma 2, $\det(\tilde{M}_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree at most L where

$$\begin{aligned} L &= \frac{1}{2}\sum_{i=1}^{m-1}\kappa_i(\kappa_i - 1) - \sum_{i=2}^{m-1}(m-i)(\kappa_i - \kappa_{i-1})\hat{\kappa}_i \\ &= \frac{1}{2}\sum_{i=2}^{m}(k - \hat{k}_i)(k - \hat{k}_i - 1) - \sum_{i=2}^{m-1}(i-1)(\hat{k}_{i+1} - \hat{k}_i)(k - k_i). \end{aligned}$$

If $\boldsymbol{u} \in \mathcal{B}_2$, (6), then for any matrix $M_{\boldsymbol{u}}$, we can obtain a matrix $\tilde{M}_{\boldsymbol{u}}$ such that $|\det(M_{\boldsymbol{u}})| = |\det(\tilde{M}_{\boldsymbol{u}})| = |\det(\tilde{M}'_{\boldsymbol{u}})|$, where $\tilde{M}'_{\boldsymbol{u}}$ is the submatrix obtained by

removing the first column and the last row of $\tilde{M}_{\boldsymbol{u}}$. In this case $\hat{k}_{m-i+1} - 1 \leq |\boldsymbol{u}([m-i])| \leq k_{m-i} - 1$ for every $i \in [m-1]$, hence

$$\hat{\kappa}_{i+1} = (k-1) - (k_{m-i} - 1) \leq |\boldsymbol{u}([m-i+1, m])| \leq (k-1) - (\hat{k}_{m-i+1} - 1) = \kappa_i$$

for every $i \in [m-1]$. Lemma 2 implies that $\det(\tilde{M}'_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree at most L too, and the claim follows. □

Now, take a finite field $\mathbb{F}_{q^\lambda}$, where $q > \max_{i \in J_m}\{n_i\}$ is a prime power and $\lambda > L$. Take all $\beta_{i,v}$ in the matrix (10) from $\mathbb{F}_q \backslash \{0\}$ and take $x \in \mathbb{F}_{q^\lambda}$ such that its minimal polynomial over $\mathbb{F}_q$ is of degree λ. Using the similar method to prove Theorem 5 and Proposition 6, we can obtain the following results.

Theorem 6. *The matrix (10) is a representation of the matroid associated to IHASs (1) over $\mathbb{F}_{q^\lambda}$ for some prime power $q > \max_{i \in J_m}\{n_i\}$ and some $\lambda > L$. Moreover, such a representation can be obtained in time $O(q, \lambda)$.*

Proposition 7. *Suppose M is the matrix (10). Then $LSSS(M)$ realizes the IHASs (1) over $\mathbb{F}_{q^\lambda}$ defined as in Theorem 6. Moreover, such a scheme can be obtained in time $O(q, \lambda)$.*

Remark 1. In some cases, Proposition 7 can give schemes for IHASs superior to the ones given by Proposition 6. For example, Proposition 6 can give the scheme for the DHTASs (2) over $\mathbb{F}_{q^\lambda}$ with $\lambda > K = \frac{1}{2}\sum_{i=1}^{m-1} k_i(k_i - 1)$ since $\hat{k}_1 = \cdots = \hat{k}_m = 0$ and the scheme for the CHTASs (3) over $\mathbb{F}_{q^\lambda}$ with $\lambda > K = \frac{1}{2}\sum_{i=1}^{m-1} k_i(k_i - 1) = \frac{1}{2}(m-1)k(k-1)$ since $0 = \hat{k}_1 < \cdots < \hat{k}_m$ and $k_1 = \cdots = k_m = k$.

On the other hand, Proposition 7 give the scheme for the DHTASs (2) over $\mathbb{F}_{q^\lambda}$ with $\lambda > L = \frac{1}{2}\sum_{i=2}^{m}(k - \hat{k}_i)(k - \hat{k}_i - 1) = \frac{1}{2}(m-1)k(k-1)$ and the scheme for the DHTASs (3) over $\mathbb{F}_{q^\lambda}$ with $\lambda > L = \frac{1}{2}\sum_{i=1}^{m-1}(k - \tilde{k}_i)(k - \tilde{k}_i - 1)$.

Therefore, Proposition 6 gives the scheme for DHTASs superior to the one given by Proposition 7. Nevertheless, Proposition 7 gives the scheme for CHTASs superior to the one given by Proposition 6.

4.3 Comparisons

Comparison to the Construction of Brickell. Brickell [9] presented an efficient method to construct the ideal linear scheme for the DHTASs (2) over $\mathbb{F}_{q^{\lambda'}}$ with $q > \max_{i \in J_m}\{n_i\}$ and $\lambda' \geq mk^2$. Proposition 6 gives a scheme for the DHTASs (2) too. In fact, our scheme is the same as Brickell's scheme. Nevertheless, Proposition 6 implies the scheme for the DHTASs (2) can be obtained over $\mathbb{F}_{q^\lambda}$ with $\lambda > K = \frac{1}{2}\sum_{i=1}^{m-1} k_i(k_i - 1)$. Therefore, we improve the bound for the field size since

$$\frac{1}{2}\sum_{i=1}^{m-1} k_i(k_i - 1) + 1 \leq \frac{1}{2}(m-1)k_{m-1}(k_{m-1} - 1) + 1 < \frac{1}{2}(m-1)k_{m-1}^2 < mk^2.$$

The reason for the improvement is that we give a relatively precise description of $\det(M_{\boldsymbol{u}})$ by the formula provided in Proposition 1.

Comparison to the Construction of Tassa. Tassa [35] presented an efficient method to construct the ideal linear scheme for the CHTAS (3) over $\mathbb{F}_p$ where

$$p > 2^{-k+2}(k-1)^{(k-1)/2}(k-1)!N^{(k-1)(k-2)/2} \tag{11}$$

is a prime and N is the maximum identity assigning to participants. Proposition 7 gives a scheme for the CHTAS (3) over $\mathbb{F}_{q^\lambda}$ with $q > \max_{i\in J_m}\{n_i\}$ and $\lambda > L = \frac{1}{2}\sum_{i=1}^{m-1}(k-\tilde{k}_i)(k-\tilde{k}_i-1)$.

Since $(k-1)! \geq 2^{k-2}$ when $k \geq 2$, it follows that the right hand of (11) is great than or equal to $(k-1)^{(k-1)/2}N^{(k-1)(k-2)/2}$. From this with $N \geq n \geq \max_{i\in J_m}\{n_i\}$, we have

$$q^L \leq N^{(k-1)(k-2)/2} < 2^{-k+2}(k-1)^{(k-1)/2}(k-1)!N^{(k-1)(k-2)/2}$$

if $L \leq \frac{1}{2}(k-1)(k-2)$. In fact, $\max_{i\in J_m}\{n_i\} \ll N$ in general. This implies in this case $2^{-k+2}(k-1)^{(k-1)/2}(k-1)!N^{(k-1)(k-2)/2} \gg q^L$, and consequently, our result is superior to Tassa's result. In the case of $L > \frac{1}{2}(k-1)(k-2)$, it is very possible that q^L is smaller than the right hand of (11). In particular, our efficient methods can also work for non-prime fields.

5 Secret Sharing Schemes for Compartmented Access Structures

In this section, we study ideal linear secret sharing schemes for two families of compartmented access structures by efficient methods.

5.1 Construction for Compartmented Access Structures with Upper Bounds

In this section, we construct ideal linear secret sharing schemes realizing UCASs. We first present a representation of the integer polymatroid $\mathcal{Z}'$ satisfying Theorem 2 such that the UCASs (5) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$.

Take $\Pi = (\Pi_i)_{i\in J_m}$ be a partition of the set P such that $|\Pi_i| = n_i$. Let $\boldsymbol{r} \in \mathbb{Z}_+^{J'_m}$ and $k \in \mathbb{N}$ such that $r_0 = 1$, $\boldsymbol{r}(J_m) \leq \Pi(P)$ and $r_i \leq k \leq |\boldsymbol{r}(J_m)|$ for every $i \in J_m$. The following result was presented in Section 8.2 of [17].

Lemma 5. *Suppose $\mathcal{Z}' = (J'_m, h)$ is an integer polymatroid such that $h(X) = \min\{k, |\boldsymbol{r}(X)|\}$ for every $X \subseteq J'_m$. Then the UCASs (5) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$.*

Now, we introduce a linear representation of the polymatroid defined in Lemma 5. Take different elements $\alpha_{i,j} \in \mathbb{F}_q$ with $i \in J'_m$ and $j \in [r_i]$, where $q \geq \max_{i\in J_m}\{n_i, |\boldsymbol{r}(J_m)|+1\}$ is a prime power. For every $i \in J'_m$, let

$$A_i = \left(\alpha_{i,v}^{u-1}\right) \qquad u \in [k],\ v \in [r_i]$$

and consider the $\mathbb{F}_q$-vector subspace $V_i \subseteq \mathbb{F}_q^k$ spanned by all the columns of A_i. Let the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ such that $h(X) = \dim\left(\sum_{i\in X} V_i\right)$ for every $X \subseteq J'_m$. We have the following result.

Proposition 8. *For the integer polymatroid $\mathcal{Z}'$ defined above, the UCASs (5) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$ and*

$$\mathcal{B}(\mathcal{Z}') = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = k \text{ and } \boldsymbol{u} \leq \boldsymbol{r}\}. \tag{12}$$

Proof. Let $A = (A_0|A_1|\cdots|A_m)$. Then it is a $k \times (|\boldsymbol{r}(J_m)| + 1)$ Vandermonde matrix. Therefore, any $k \times k$ submatrix of A is nonsingular. This with $\dim(V_i) = r_i$ for every $i \in J'_m$ implies the second claim. In addition, $\left|\bigcup_{i\in X}\{\boldsymbol{a_{i,v}} : v \in [r_i]\}\right| = |\boldsymbol{r}(X)|$ for every $X \subseteq J'_m$ where $\boldsymbol{a_{i,v}}$ denotes the vth columns of A_i. Hence, $h(X) = \min\left\{k, |\boldsymbol{r}(X)|\right\}$ for every $X \subseteq J'_m$, and the first claim follows. □

This proposition implies that the collection $(V_i)_{i\in J'_m}$ is a linear representation of the integer polymatroid $\mathcal{Z}'$ associated to the UCASs (5). We next present a matrix M based on $\mathcal{Z}'$, which is a representation of a matroid $\mathcal{M}$ such that the UCASs (5) are of the form $\Gamma_{p_0}(\mathcal{M})$.

Let $\Pi_0 = \{p_0\}$ and let $\Pi' = (\Pi_i)_{i\in J'_m}$ and $\Pi = (\Pi_i)_{i\in J_m}$ be the partition of $P' = P \cup \{p_0\}$ and P, respectively, such that $|\Pi_i| = n_i$. For every $i \in J'_m$, take n_i different elements $\beta_{i,v} \in \mathbb{F}_q$ with $v \in [n_i]$ and let

$$B_i = \left((\beta_{i,v}x)^{u-1}\right) \qquad u \in [r_i],\ v \in [n_i].$$

Let a $k \times (n+1)$ matrix be defined as

$$M = (M_0|M_1|\cdots|M_m) \tag{13}$$

where $M_i = A_iB_i$. We have the following result.

Lemma 6. *For any $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, (12), $\det(M_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree at most $k(r-1)$, where $r = \max_{i\in J_m}\{r_i\}$.*

Proof. Without loss of generality, we may assume that $M_{\boldsymbol{u}}$ is the $k\times k$ submatrix of M formed by the first u_i columns in every M_i. For every $i \in J'_m$, take $\bar{B}_i = \left(\beta_{i,v}^{u-1}\right)$ with $u \in [r_i]$ and $v \in [n_i]$, and let B'_i and $\bar{B}'_i$ denote the submatrices formed by the first u_i columns in B_i and $\bar{B}_i$, respectively. In addition, for any $\boldsymbol{j_i} = (j_{i,1}, \ldots, j_{i,u_i})$ with $i \in J'_m$ such that $1 \leq j_{i,1} < \cdots < j_{i,u_i} \leq r_i$, let $B'_i(\boldsymbol{j_i})$ and $\bar{B}'_i(\boldsymbol{j_i})$ denote the $u_i \times u_i$ submatrices formed by the $j_{i,1}$th row, …, j_{i,u_i}th row of B'_i and $\bar{B}'_i$, respectively, and let $A_i(\boldsymbol{j_i})$ denote the submatrix formed by the first u_i columns in A_i. Then

$$\det\left(B'_i(\boldsymbol{j_i})\right) = \det\left(\bar{B}'_i(\boldsymbol{j_i})\right)x^{\sum_{v=1}^{u_i}(j_{i,v}-1)}.$$

If $j_{i,v} = r_i - u_i + v$ for $v \in [u_i]$, then the exponent of x in $\det(B'_i(\boldsymbol{j_i}))$ is maximum, that is

$$\sum_{v=1}^{u_i}(j_{i,v}-1) = \sum_{v=1}^{u_i}(r_i-u_i+v-1) = u_i(r_i-u_i) + \sum_{v=1}^{u_i-1} v = \frac{1}{2}u_i(2r_i-u_i-1). \tag{14}$$

Note that in this case $\bar{B}'_i(\boldsymbol{j_i})$ is the submatrix formed by of the last u_i rows of $\bar{B}'_i$, it follows $\det(\bar{B}'_i(\boldsymbol{j_i})) \neq 0$. Hence, Proposition 4 implies that $\det(M_{\boldsymbol{u}})$ can be

viewed as a polynomial on x and the summation with maximum exponent of x in it is

$$\Big(\prod_{i=1}^{m} \det\left(\bar{B}_i'(\boldsymbol{j_i})\right)\Big) \det\Big(\big(A_0(\boldsymbol{j_0})|A_1(\boldsymbol{j_1})|\cdots|A_m(\boldsymbol{j_m})\big)\Big)x^t, \tag{15}$$

where for $i \in J_m$ and $v \in [u_i]$, $j_{i,v} = r_i - u_i + v$. As $\sum_{i=1}^m u_i^2 \geq \sum_{i=1}^m u_i$ and $\sum_{i=1}^m u_i = k$ or $k-1$, from (14), we have

$$t = \frac{1}{2}\sum_{i=1}^{m} u_i(2r_i - u_i - 1) = \sum_{i=1}^{m} u_i r_i - \frac{1}{2}\sum_{i=1}^{m}(u_i^2 + u_i) \leq k(r-1). \tag{16}$$

In addition, the matrix $\big(A_0(\boldsymbol{j_0})|A_1(\boldsymbol{j_1})|\cdots|A_m(\boldsymbol{j_m})\big)$ is nonsingular, thus $\det(M_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree t. Using the same method, we can prove this claim for any $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, (12). □

Now, take a finite field $\mathbb{F}_{q^\lambda}$, where $q \geq \max_{i\in J_m}\{n_i, |\boldsymbol{r}(J_m)|+1\}$ is a prime power and $\lambda > k(r-1)$. Take $\alpha_{i,v}$ and $\beta_{i,v}$ in the matrix (13) from $\mathbb{F}_q$ and take $x \in \mathbb{F}_{q^\lambda}$ such that its minimal polynomial over $\mathbb{F}_q$ is of degree λ. Then similar to Theorem 5 and Proposition 6, from this lemma, we can obtain the following result.

Theorem 7. *The matrix (13) is a representation of the matroid associated to UCASs (5) over $\mathbb{F}_{q^\lambda}$ for some prime power $q \geq \max_{i\in J_m}\{n_i, |\boldsymbol{r}(J_m)|+1\}$ and some $\lambda > k(r-1)$. Moreover, such a representation can be obtained in time $O(q, \lambda)$.*

Proposition 9. *Suppose M is the matrix (13). Then $LSSS(M)$ realizes the UCASs (5) over $\mathbb{F}_{q^\lambda}$ defined as in Theorem 7. Moreover, such a scheme can be obtained in time $O(q, \lambda)$.*

Proof. If $\boldsymbol{u}(J_m) \in \min \Gamma$ and $u_0 = 0$, then $\boldsymbol{u}(J_m') \in \mathcal{B}(\mathcal{Z}')$, (12). Theorem 7 implies $M_{\boldsymbol{u}(J_m)}$ is nonsingular. Accordingly, M_0 can be spanned by the columns in $M_{\boldsymbol{u}(J_m)}$ for any $\boldsymbol{u}(J_m) \in \Gamma$. Assume that $\boldsymbol{u}(J) \notin \Gamma$. As $h(\{(i)\}) = r_i$ for every $i \in J_m$, thus without loss of generality, we may assume that $\boldsymbol{u}(J_m) \leq \boldsymbol{r}(J_m)$. Furthermore, we may assume that $|\boldsymbol{u}(J_m)| = k-1$, since if $|\boldsymbol{u}(J_m)| < k-1$, we may find a vector $\boldsymbol{u'}(J_m) \geq \boldsymbol{u}(J_m)$ such that $\boldsymbol{u'}(J_m) \leq \boldsymbol{r}(J_m)$ and $|\boldsymbol{u'}(J_m)| = k-1$. In this case if $u_0 = 1$, then $\boldsymbol{u}(J_m') \in \mathcal{B}(\mathcal{Z}')$. Theorem 7 implies $M_{\boldsymbol{u}(J_m')}$ is nonsingular, and the claim follows. □

5.2 Construction for Compartmented Access Structures with Lower Bounds

In this section, we describe ideal linear secret sharing schemes realizing LCASs based on the schemes for the dual access structures of LCASs.

The dual access structures of LCASs (4) presented in [37] are defined as

$$\Gamma^* = \{\boldsymbol{u} \in \mathbf{P} : |\boldsymbol{u}| \geq l \text{ or } u_i \geq \tau_i \text{ for some } i \in J_m\} \tag{17}$$

where $l = |P| - k + 1$, $\tau_i = |\Pi_i| - t_i + 1$ for $i \in J$, and $|\boldsymbol{\tau}| \geq l + m - 1$.

We first present a representation of the integer polymatroid $\mathcal{Z}'$ satisfying Theorem 2 such that the access structures (17) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$.

Take $\Pi = (\Pi_i)_{i \in J_m}$ be a partition of the set P such that $|\Pi_i| = n_i$. Let $\boldsymbol{\tau} \in \mathbb{Z}_+^{J'_m}$ and $l \in \mathbb{N}$ such that $\tau_0 = 1$, $\boldsymbol{\tau}(J_m) \leq \Pi(P)$ and $|\boldsymbol{\tau}(J_m)| \geq l + m - 1$. Take $\boldsymbol{\tau'} \in \mathbb{Z}_+^{J'_m}$ such that $\tau'_0 = 1$ and $\tau'_i = \tau_i - 1$ for every $i \in J_m$. The following result was presented in Section IV-D of [19].

Lemma 7. *Suppose $\mathcal{Z}' = (J'_m, h)$ is an integer polymatroid with h satisfying*

(1) $h(\{0\}) = 1$;
(2) $h(X) = \min\{l, 1 + |\boldsymbol{\tau'}(X)|\}$ for every $X \subseteq J_m$;
(3) $h(X \cup \{0\}) = h(X)$ for every $X \subseteq J_m$.

Then the access structures (17) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$.

We next introduce a linear representation of the polymatroid defined in Lemma 7. Take elements $\alpha_{i,j} \in \mathbb{F}_q$ with $i \in J'_m$ and $j \in [\tau_i]$ where $q > \max_{i \in J_m}\{n_i, |\boldsymbol{\tau'}(J_m)|\}$ is a prime power such that

- $\alpha_{i,1} = \alpha_0$ for all $i \in J'_m$ and
- the elements α_0 and $\alpha_{i,j}$ with $i \in J_m$ and $j \in [2, \tau_i]$ are pairwise distinct.

For every $i \in J'_m$, let

$$A_i = \left(\alpha_{i,v}^{u-1}\right) \qquad u \in [l],\ v \in [\tau_i]$$

and consider the $\mathbb{F}_q$-vector subspace $V_i \subseteq \mathbb{F}_q^k$ spanned by all the columns of A_i. Let the integer polymatroid $\mathcal{Z}' = (J'_m, h)$ such that $h(X) = \dim\left(\sum_{i \in X} V_i\right)$ for every $X \subseteq J'_m$.

Proposition 10. *For the integer polymatroid $\mathcal{Z}'$ defined above, the access structures (17) are of the form $\Gamma_0(\mathcal{Z}', \Pi)$ and $\mathcal{B}(\mathcal{Z}') = \mathcal{B}_1 \cup \mathcal{B}_2$, where*

$$\begin{aligned} \mathcal{B}_1 = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = l,\ u_0 = 0,\ u_{i'} \leq \tau_{i'} \text{ for some } i' \in J_m \\ \text{and } u_i \leq \tau'_i \text{ for all } i \in J_m \backslash \{i'\}\}, \\ \mathcal{B}_2 = \{\boldsymbol{u} \in \mathbb{Z}_+^{J'_m} : |\boldsymbol{u}| = l,\ u_0 = 1 \text{ and } \boldsymbol{u}(J_m) \leq \boldsymbol{\tau'}(J_m)\}. \end{aligned} \tag{18}$$

Proof. Proving the first claim is equivalent to proving that h satisfies the three conditions in Lemma 7. First, $h(\{0\}) = 1$ as $\dim(V_0) = 1$. Let A be the matrix formed by the column A_0 and the last τ'_i columns of A_i for every $i \in J_m$. Then it is a $l \times (1 + |\boldsymbol{\tau'}(J_m)|)$ Vandermonde matrix. Accordingly, any $l \times l$ submatrix of A is nonsingular. Since $\left|\bigcup_{i \in X}\{\boldsymbol{a_{i,v}} : v \in [\tau_i]\}\right| = 1 + |\boldsymbol{\tau'}(X)|$ for every $X \subseteq J_m$ where $\boldsymbol{a_{i,v}}$ denotes the vth columns of A_i, it follows that $h(X) = \min\{l, 1 + |\boldsymbol{\tau'}(X)|\}$ for every $X \subseteq J_m$. Moreover, $V_0 \subseteq V_i$ for every $X \subseteq J_m$, Therefore, $h(X \cup \{0\}) = h(X)$ for every $X \subseteq J_m$.

In addition, since any $l \times l$ submatrix of A is nonsingular, on the one hand, any l distinct columns from A_i with $i \in J_m$ are linearly independent, and on the other hand, A_0 and any $l - 1$ columns from the last τ'_i columns of A_i with $i \in J_m$ are linearly independent too. This implies the second claim. □

We next present a matrix M which is a representation of a matroid $\mathcal{M}$ such that the access structures (17) are of the form $\Gamma_{p_0}(\mathcal{M})$.

Suppose $\Pi_0 = \{p_0\}$ and let $\Pi' = (\Pi_i)_{i\in J'_m}$ and $\Pi = (\Pi_i)_{i\in J_m}$ be the partition of $P' = P \cup \{p_0\}$ and P, respectively, such that $|\Pi_i| = n_i$. Take $\beta_{0,1} = 0$ and for every $i \in J_m$, take n_i different elements $\beta_{i,v} \in \mathbb{F}_q$ with $v \in [n_i]$ such that $\beta_{i,v} \neq 0$. For every $i \in J'_m$, take

$$B_i = \left((\beta_{i,v}x)^{u-1}\right) \qquad u \in [\tau_i],\ v \in [n_i]$$

and $M_i = A_iB_i$. Define a $l \times (n+1)$ matrix as

$$M = (M_0|M_1|\cdots|M_m). \tag{19}$$

Lemma 8. *For any $\boldsymbol{u} \in \mathcal{B}(\mathcal{Z}')$, (18), $\det(M_{\boldsymbol{u}})$ is a nonzero polynomial on x of degree at most $l(\tau-1)$, where $\tau = \max_{i\in J_m}\{\tau_i\}$.*

Proof. Without loss of generality, we may assume that $M_{\boldsymbol{u}}$ is the $l\times l$ submatrix of M formed by the first u_i columns in every M_i. For every $i \in J'_m$, take $\bar{B}_i = \left(\beta_{i,v}^{u-1}\right)$ with $u \in [\tau_i]$ and $v \in [n_i]$, and let $\bar{B}'_i$ denote the submatrix formed by the first u_i columns in $\bar{B}_i$. Proposition 4 implies that $\det(M_{\boldsymbol{u}})$ can be viewed as a polynomial on x.

In the case of $\boldsymbol{u} \in \mathcal{B}_1$, let the summation with maximum exponent of x in $\det(M_{\boldsymbol{u}})$ be denoted by $a_{t_1}x^{t_1}$. Then similar to (15),

$$a_{t_1}x^{t_1} = \Big(\prod_{i=1}^{m}\det\left(\bar{B}'_i(\boldsymbol{j_i})\right)\Big)\det\left(\left(A_1(\boldsymbol{j_1})|\cdots|A_m(\boldsymbol{j_m})\right)\right)x^{t_1},$$

where $\boldsymbol{j_i} = (j_{i,1},\ldots,j_{i,u_i})$ with $i \in J_m$ such that $j_{i,v} = \tau_i - u_i + v$ for $v \in [u_i]$. In this case the matrix $\left(A_1(\boldsymbol{j_1})|\cdots|A_m(\boldsymbol{j_m})\right)$ is nonsingular since its all columns are pairwise distinct. From this and each $\bar{B}'_i(\boldsymbol{j_i})$ is nonsingular, we have that $a_{t_1} \neq 0$. In addition, as $u_i \leq \tau_i$ for every $i \in J_m$, the inequality (16) implies $t_1 \leq l(\tau-1)$.

In the case of $\boldsymbol{u} \in \mathcal{B}_2$, let the summation with maximum exponent of x in $\det(M_{\boldsymbol{u}})$ be denoted by $a_{t_2}x^{t_2}$. Then

$$a_{t_2}x^{t_2} = \Big(\prod_{i=1}^{m}\det\left(\bar{B}'_i(\boldsymbol{j_i})\right)\Big)\det\left(\left(A_0|A_1(\boldsymbol{j_1})|\ldots|A_m(\boldsymbol{j_m})\right)\right)x^{t_2},$$

where $\boldsymbol{j_i} = (j_{i,1},\ldots,j_{i,u_i})$ with $i \in J_m$ such that $j_{i,v} = \tau_i - u_i + v$ for $v \in [u_i]$. In this case $u_i \leq \tau_i - 1$ for every $i \in J_m$. Therefore, from the inequality (16), $t_2 \leq l(\tau-1)$. Moreover, $a_{t_2} \neq 0$ as $\bar{B}'_i(\boldsymbol{j_i})$ with $i \in J'_m$ and $\left(A_0(\boldsymbol{j_0})|\cdots|A_m(\boldsymbol{j_m})\right)$ are all nonsingular. □

Now, take a finite field $\mathbb{F}_{q^\lambda}$ with $q > \max_{i\in J_m}\{n_i, |\boldsymbol{\tau'}(J_m)|\}$ is a prime power and $\lambda > l(\tau-1)$. Take $\alpha_{i,v}$ and $\beta_{i,v}$ in the matrix (19) from $\mathbb{F}_q\backslash\{0\}$ and take $x \in \mathbb{F}_{q^\lambda}$ such that its minimal polynomial over $\mathbb{F}_q$ is of degree λ. Similar to Theorem 7, we can obtain the following result.

Theorem 8. *The matrix (19) is a representation of the matroid associated to access structures (17) over* $\mathbb{F}_{q^\lambda}$ *for some prime power* $q > \max_{i\in J_m}\{n_i, |\boldsymbol{\tau}'(J_m)|\}$ *and some* $\lambda > l(\tau-1)$. *Moreover, such a representation can be obtained in time* $O(q,\lambda)$.

Proposition 11. *Suppose* M *is the matrix (19). Then* $LSSS(M)$ *realizes the access structures (17) over* $\mathbb{F}_{q^\lambda}$ *defined as in Theorem 8. Moreover, such a scheme can be obtained in time* $O(q,\lambda)$.

Proof. Let $\boldsymbol{u}(J_m) \in \Gamma^*$, (17), be a minimal set, then $|\boldsymbol{u}(J_m)| = l$ and $\boldsymbol{u}(J_m) \leq \boldsymbol{\tau}'(J_m)$, or $u_i = \tau_i$ for some $i \in J_m$. In the first case, Theorem 8 implies M_0 is can be spanned by all the columns in $M_{\boldsymbol{u}(J_m)}$. Moreover, Theorem 8 implies any τ_i columns of M_i are linearly independent. From this with $h(\{0,i\}) = h(\{i\}) = \tau_i$ for every $i \in J_m$, M_0 is a linear combination of any τ_i columns in M_i. Hence, in the second case M_0 can be spanned by all the columns in $M_{\boldsymbol{u}(J_m)}$ too.

Assume that $\boldsymbol{u}(J_m) \notin \Gamma^*$, (17). Then $\boldsymbol{u}(J_m) \leq \boldsymbol{\tau}'(J_m)$ and $|\boldsymbol{u}(J_m)| \leq l-1$. Without loss of generality, we may assume that $|\boldsymbol{u}(J_m)| = l-1$, since if $|\boldsymbol{u}(J_m)| < l-1$, we may find a vector $\boldsymbol{u}'(J_m) \geq \boldsymbol{u}(J_m)$ such that $\boldsymbol{u}'(J_m) \leq \boldsymbol{\tau}'(J_m)$ and $|\boldsymbol{u}'(J_m)| = l-1$. As $l \leq |\boldsymbol{\tau}'(J_m)|+1$, the above-described procedure is possible. In this case if $u_0 = 1$, then $\boldsymbol{u}(J'_m) \in \mathcal{B}_2$. Theorem 8 implies $M_{\boldsymbol{u}(J'_m)}$ is nonsingular, and the claim follows. □

Remark 2. From the dual relationship of the access structures (17) and the LCASs (4), we can translate the scheme in Proposition 11 into an ideal linear scheme for the LCASs (4) using the explicit transformation of [20]. Specially, the efficient construction of ideal linear schemes realizing LCASs (4) can be obtained over $\mathbb{F}_{q^\lambda}$ in time $O(q,\lambda)$ for some prime power $q > \max_{i\in J_m}\{n_i, \sum_{i=1}^{m}(n_i - t_i)\}$ and some $\lambda > (n-k+1)t$, where $t = \max_{i\in J_m}\{n_i - t_i\}$.

Acknowledgements. The authors would like to thank the reviewers for their helpful comments and suggestions. This research was supported in part by the Foundation of National Natural Science of China (No. 61772147, 61702124), Guangdong Province Natural Science Foundation of major basic research and Cultivation project (No. 2015A030308016), Project of Ordinary University Innovation Team Construction of Guangdong Province (No. 2015KCXTD014), Collaborative Innovation Major Projects of Bureau of Education of Guangzhou City (No. 1201610005) and National Cryptography Development Fund (No. MMJJ20170117).

References

1. Ball, S., Padró, C., Weiner, Z., Xing, C.: On the representability of the biuniform matroid. SIAM J. Discrete Math. **27**(3), 1482–1491 (2013)
2. Beimel, A.: Secret-sharing schemes: a survey. In: Chee, Y.M., et al. (eds.) IWCC 2011. LNCS, vol. 6639, pp. 11–46. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20901-7_2
3. Beimel, A., Chor, B.: Universally ideal secret sharing schemes. IEEE Trans. Inf. Theory **40**(3), 786–794 (1994)

4. Beimel, A., Tassa, T., Weinreb, E.: Characterizing ideal weighted threshold secret sharing. SIAM J. Discrete Math. **22**(1), 360–397 (2008)
5. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for noncryptographic fault-tolerant distributed computations. In: Proceedings of the 20th ACM Symposium on the Theory of Computing, pp. 1–10 (1988)
6. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 27–35. Springer, New York (1990). https://doi.org/10.1007/0-387-34799-2_3
7. Beutelspacher, A., Wettl, F.: On 2-level secret sharing. Des. Codes Cryptogr. **3**(2), 127–134 (1993)
8. Blakley, G.R.: Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference 1979, AFIPS Proceedings, vol. 48, pp. 313–317 (1979)
9. Brickell, E.F.: Some ideal secret sharing schemes. J. Combin. Maths. Combin. Comp. **9**, 105–113 (1989)
10. Brickell, E.F., Davenport, D.M.: On the classification of ideal secret sharing schemes. J. Cryptol. **4**, 123–134 (1991)
11. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols. In: Proceedings of the 20th ACM Symposium on the Theory of Computing, pp. 11–19 (1988)
12. Chor, B., Kushilevitz, E.: Secret sharing over infinite domains. J. Cryptol. **6**(2), 87–96 (1993)
13. Collins, M.J.: A note on ideal tripartite access structures. Cryptology ePrint Archive, Report 2002/193. http://eprint.iacr.org/2002/193
14. Cramer, R., Damgård, I., Maurer, U.: General secure multi-party computation from any linear secret-sharing scheme. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 316–334. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_22
15. Cramer, R., et al.: On codes, matroids and secure multi-party computation from linear secret sharing schemes. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 327–343. Springer, Heidelberg (2005). https://doi.org/10.1007/11535218_20
16. Desmedt, Y., Frankel, Y.: Threshold cryptosystems. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 307–315. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_28
17. Farràs, O., Martí-Farré, J., Padró, C.: Ideal multipartite secret sharing schemes. J. Cryptol. **25**(3), 434–463 (2012)
18. Farràs, O., Padró, C.: Ideal hierarchical secret sharing schemes. IEEE Trans. Inf. Theory **58**(5), 3273–3286 (2012)
19. Farràs, O., Padró, C., Xing, C., Yang, A.: Natural generalizations of threshold secret sharing. IEEE Trans. Inf. Theory **60**(3), 1652–1664 (2014)
20. Fehr, S.: Efficient construction of the dual span program. Manuscript, May (1999)
21. Giulietti, M., Vincenti, R.: Three-level secret sharing schemes from the twisted cubic. Discrete Math. **310**(22), 3236–3240 (2010)
22. Herranz, J., Sáez, G.: New results on multipartite access structures. IEE Proc. Inf. Secur. **153**(4), 153–162 (2006)
23. Herzog, J., Hibi, T.: Discrete polymatroids. J. Algebraic Combinat. **16**(3), 239–268 (2002)
24. Ito, M., Saito, A., Nishizeki, T.: Secret sharing schemes realizing general access structure. In: Proceedings of the IEEE Global Telecommunication Conference, Globecom 1987, pp. 99–102 (1987)

25. Kothari, S.C.: Generalized linear threshold scheme. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 231–241. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_19
26. Massey, J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory, pp. 276–279 (1993)
27. Massey, J.L.: Some applications of coding theory in cryptography. Codes and Ciphers: Cryptography and Coding IV, pp. 33–47 (1995)
28. Oxley, J.G.: Matroid Theory. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York (1992)
29. Padró, C., Sáez, G.: Secret sharing schemes with bipartite access structure. IEEE Trans. Inf. Theory **46**(7), 2596–2604 (2000)
30. Schrijver, A.: Combinatorial Optimization. Polyhedra and Efficiency. Springer, Berlin (2003)
31. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
32. Shankar, B., Srinathan, K., Rangan, C.P.: Alternative protocols for generalized oblivious transfer. In: Rao, S., Chatterjee, M., Jayanti, P., Murthy, C.S.R., Saha, S.K. (eds.) ICDCN 2008. LNCS, vol. 4904, pp. 304–309. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77444-0_31
33. Shoup, V.: New algorithm for finding irreducible polynomials over finite fields. Math. Comput. **54**, 435–447 (1990)
34. Simmons, G.J.: How to (really) share a secret. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 390–448. Springer, New York (1990). https://doi.org/10.1007/0-387-34799-2_30
35. Tassa, T.: Hierarchical threshold secret sharing. J. Cryptol. **20**(2), 237–264 (2007)
36. Tassa, T.: Generalized oblivious transfer by secret sharing. Des. Codes Cryptol. **58**(1), 11–21 (2011)
37. Tassa, T., Dyn, N.: Multipartite secret sharing by bivariate interpolation. J. Cryptol. **22**(2), 227–258 (2009)
38. Welsh, D.J.A.: Matroid Theory. Academic Press, London (1976)