Natural Generalizations of Threshold Secret Sharing

Oriol Farràs[1], Carles Padró[2], Chaoping Xing[2], and An Yang[2]*

[1] Universitat Rovira i Virgili, Tarragona, and Ben Gurion University, Be'er Sheva
[2] Nanyang Technological University, Singapore
oriol.farras@urv.cat, {carlespl, xingcp, yang0246}@ntu.edu.sg

Abstract. We present new families of access structures that, similarly to the multilevel and compartmented access structures introduced in previous works, are natural generalizations of threshold secret sharing. Namely, they admit an ideal linear secret sharing schemes over every large enough finite field, they can be described by a small number of parameters, and they have useful properties for the applications of secret sharing. The use of integer polymatroids makes it possible to find many new such families and it simplifies in great measure the proofs for the existence of ideal secret sharing schemes for them.

Key words. Cryptography, secret sharing, ideal secret sharing schemes, multipartite secret sharing, integer polymatroids.

1 Introduction

The first proposed secret sharing schemes by Shamir [29] and by Blakley [6] have *threshold access structures*, that is, the qualified subsets are those having at least a certain number of participants. In addition, they are *ideal*, which means that every share has the same length as the secret. Moreover, as it was noticed by Bloom [7] and by Karnin, Greene and Hellman [19], they are *linear*, which implies that both the computation of the shares and the reconstruction of the secret can be performed by using basic linear algebra operations.

Even though there exists a linear secret sharing scheme for every access structure [4, 18], the known general constructions are very inefficient 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. Readers are referred to [2] for a recent survey on this topic.

Nevertheless, this does not mean that efficient secret sharing schemes exist only for threshold access structures. Actually, the construction of ideal linear

* The work of the first author was supported by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES" and by the Government of Catalonia through grant 2009 SGR 1135, and by ISF grant 938/09. The work of the other authors was supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

secret sharing schemes for non-threshold access structures has attracted a lot of attention. This line of research was initiated by Kothari [20], who presented some ideas to construct ideal linear secret sharing schemes with hierarchical properties. Simmons [30] introduced the multilevel and compartmented access structures, and presented geometric constructions of ideal linear secret sharing schemes for some of them. Brickell [8] formalized the ideas in previous works [7, 19, 20, 30] and introduced a powerful linear-algebraic method to construct ideal linear secret sharing schemes for non-threshold access structures. In addition, he used that method to construct such schemes for the families of access structures introduced by Simmons [30]. Tassa [31] and Tassa and Dyn [32] combined Brickell's [8] method with different kinds of polynomial interpolation to construct ideal linear secret sharing schemes for more general families of multilevel and compartmented access structures. Constructions for other interesting variants of compartmented access structures are given in [16, 23]. All these families of access structures have some common features that are enumerated in the following.

1. They are natural and useful generalizations of threshold access structures. In the threshold case, all participants are equivalent, while the access structures in those families are *multipartite*, which means that the participants are divided into several parts and the participants in the same part play an equivalent role in the structure. In addition, they have some interesting properties for the applications of secret sharing. Some of them are useful for hierarchical organizations, while others can be used in situations requiring the agreement of several parties.
2. Similarly to the threshold ones, the access structures in those families admit a very compact description. Typically, they can be described by using a small number of parameters, at most linear on the number of parts.
3. They are *ideal access structures*, that is, they admit an ideal secret sharing scheme. Actually, every one of those access structures admits a *vector space secret sharing scheme*, that is, an ideal linear secret sharing scheme constructed by using the method proposed by Brickell [8]. Moreover, the only restriction on the fields over which these schemes are constructed is their size, and hence there is no required condition about their characteristic. Observe that this is also the case for threshold access structures, which admit vector space secret sharing schemes over every finite field with at least as many elements as the number of participants.
4. Even though the existence of ideal linear secret sharing schemes for those access structures has been proved, the known methods to construct such schemes are not efficient in general. This is an important difference to the threshold case, in which the construction proposed by Shamir [29] solves the problem. Tassa [31, Section 3.3] presented an efficient algorithm for the multilevel access structures. This is the only other family for which an efficient algorithm is known.
5. Determining over which fields those schemes can be constructed is another open problem. It is unsolved even for threshold access structures. In this case, it is equivalent to the problem considered in [1], and it is equivalent as well to

determine over which fields uniform matroids are representable [24, Problem 6.5.12, Conjecture 14.1.5], and also to determine the size of maximum arcs in projective spaces [27]. This is due to the well-known connection between threshold secret sharing and maximum distance separable codes [22]. Much less is known for the other families of multipartite access structures. Differently to the threshold case, there is a huge gap between the known lower and upper bounds on the minimum size of such fields.

Two questions naturally arise at this point. The first one is the search for new families of access structures with the properties above. The second one is to determine the existence of efficient methods to construct ideal linear secret sharing schemes for them, and to find better bounds on the minimum size of the fields over which such schemes can be found.

Another related line of work deals with the characterization of the ideal access structures in several families of multipartite access structures. The bipartite access structures [25] and the weighted threshold access structures [3] were the first families for which such a characterization was given. Some partial results about the tripartite case were presented in [10, 16]. On the basis of the well known connection between ideal secret sharing schemes and matroids [9], Farràs, Martí-Farré and Padró [12] introduced integer polymatroids to study ideal multipartite secret sharing schemes. The power of this new mathematical tool was demonstrated in the same work by using it to characterize the ideal tripartite access structures. Subsequently, the use of integer polymatroids made it possible to characterize the ideal hierarchical access structures [14].

This work is devoted to the search for new families of ideal access structures that are among the most natural generalizations of threshold secret sharing, and to the efficiency analysis of the methods to construct ideal secret sharing schemes for them.

Our results strongly rely on the connection between integer polymatroids and ideal multipartite secret sharing presented in [12], which is summarized here in Theorem 2.2. The concepts, notation and related facts that are required to understand this result are recalled Section 2. Actually, the use of this tool provides important advantages in comparison to the techniques applied in previous constructions of ideal multipartite secret sharing schemes [8, 16, 23, 25, 30–32].

While no strong connection between all those families was previously known, a remarkable common feature is made apparent by identifying the integer polymatroids that are associated to those ideal multipartite access structures. Namely, they are Boolean polymatroids or basic transformations and combinations of Boolean polymatroids. This is of course a fundamental clue when trying to find new families of ideal access structures satisfying the aforementioned requirements.

By using other Boolean polymatroids, and by combining them in several different ways, we present a number of new families of ideal multipartite access structures. Specifically, we present in Section 4 several generalizations of the compartmented access structures introduced in [8, 30, 32]. Section 5 deals with some families of partially hierarchical access structures that can be defined from Boolean polymatroids. For instance, we present a family of compartmented access structures in which every compartment has a hierarchy. Ideal (totally) hierarchical access structures, which were completely characterized in [14], are associated as well to a special class of Boolean polymatroids. Finally, we use another family of integer polymatroids, the uniform ones, to characterize in Section 6 the ideal members of another family of multipartite access structures: the ones that are invariant under every permutation of the parts.

All integer polymatroids that we use to find new families of ideal multipartite access structures can be defined by a small number of parameters, linear on the size of the ground set, and they are representable over every large enough finite field. Actually, these requirements are implied by the conditions we imposed on the access structures to be simple generalizations of threshold secret sharing. We analyze in Section 3 the basic integer polymatroids as well as the operations to modify and combine them that are used in our constructions. In particular, the result we prove in Proposition 3.4 is extremely useful.

We focus in this paper on a few examples that can be useful for the applications of secret sharing, but many other families can be described by using other integer polymatroids with those properties, and surely some other useful families will be found in future works.

Differently to the aforementioned previous works, our proofs that the structures in these new families are ideal are extremely concise. Of course, this is due to the use of integer polymatroids. In addition, some easily checkable necessary conditions that are derived from the results in [12] make it possible to prove that certain given multipartite access structures are not ideal. This simplifies as well the search for new families.

Even though the efficiency of the methods to construct actual ideal linear secret sharing schemes for those families of access structures has not been significantly improved by using the results from [12], they provide a unified framework in which the open problems related to that issue can be precisely stated. These open problems and some possible strategies to attack them are discussed in Section 7.

2 Preliminaries

2.1 Multipartite Access Structures and Their Geometric Representation

We introduce here some notation that will be used all through the paper. In addition, we present a very useful geometric representation of multipartite access structures that was introduced in [12, 25].

We use $\mathbb{Z}_+$ to denote the set of the non-negative integers. For every $i, j \in \mathbb{Z}$ we write $[i, j] = \{i, i+1, \ldots, j\}$ if $i < j$, while $[i, i] = \{i\}$ and $[i, j] = \emptyset$ if $i > j$. Consider a finite set J. We notate J' for a set of the form $J' = J \cup \{p_0\}$ for some $p_0 \notin J$. Given two vectors $u = (u_i)_{i \in J}$ and $v = (v_i)_{i \in J}$ in $\mathbb{Z}^J$, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J$. The *modulus* $|u|$ of a vector $u \in \mathbb{Z}_+^J$ is defined by $|u| = \sum_{i \in J} u_i$. For every subset $X \subseteq J$, we notate $u(X) = (u_i)_{i \in X} \in \mathbb{Z}^X$. The *support of* $u \in \mathbb{Z}^J$ is defined as $\operatorname{supp}(u) = \{i \in J : u_i \neq 0\}$. Finally, we consider the vectors $\mathbf{e}^i \in \mathbb{Z}^J$ such that $\mathbf{e}^i_j = 1$ if $j = i$ and $\mathbf{e}^i_j = 0$ otherwise.

For a finite set P, we notate $\mathcal{P}(P)$ for the power set of P, that is, the set of all subsets of P. A family $\Pi = (\Pi_i)_{i \in J}$ of subsets of P is called here a *partition of* P if $P = \bigcup_{i \in J} \Pi_i$ and $\Pi_i \cap \Pi_j = \emptyset$ whenever $i \neq j$. Observe that some of the parts may be empty. If $|J| = m$, we say that Π is an *m-partition* of P. For a partition Π of a set P, we consider the mapping $\Pi \colon \mathcal{P}(P) \to \mathbb{Z}^J_+$ defined by $\Pi(A) = (|A \cap \Pi_i|)_{i \in J}$. We write $\mathbf{P} = \Pi(\mathcal{P}(P)) = \{u \in \mathbb{Z}^J_+ : u \leq (|\Pi_i|)_{i \in J}\}$. 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. If the number of parts in Π is m, such an access structure is called *m-partite*.

A multipartite access structure can be described 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 $A \in \Gamma$ if and only if $\Pi(A) \in \Pi(\Gamma)$. That is, Γ is completely determined by the partition Π and set of vectors $\Pi(\Gamma) \subseteq \mathbf{P} \subseteq \mathbb{Z}^J_+$. Moreover, the set $\Pi(\Gamma) \subseteq \mathbf{P}$ is monotone increasing, that is, if $u \in \Pi(\Gamma)$ and $v \in \mathbf{P}$ are such that $u \leq v$, then $v \in \Pi(\Gamma)$. 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 P, and the same applies to $\min \Gamma$.

2.2 Polymatroids and Matroids

A *polymatroid* $\mathcal{S}$ is a pair (J, h) formed by a finite set J, the *ground set*, and a *rank function* $h \colon \mathcal{P}(J) \to \mathbb{R}$ satisfying

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

If the rank function h is integer-valued, we say that $\mathcal{S}$ is an *integer polymatroid*. An integer polymatroid such that $h(X) \leq |X|$ for every $X \subseteq J$ is called a *matroid*. Readers that are unfamiliar with Matroid Theory are referred to the textbooks [24, 33]. A detailed presentation about polymatroids can be found in [28, Chapter 44] or [17].

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. Let V be a $\mathbb{K}$-vector space, and let $(V_i)_{i \in J}$ be a finite collection of subspaces of V. It is not difficult to check that the mapping $h \colon \mathcal{P}(J) \to \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i \in X} V_i)$ is the rank function of an integer polymatroid. Integer polymatroids and, in particular, matroids that can be defined in this way are said to be $\mathbb{K}$*-representable*. Observe that, in a representable matroid, $\dim V_i \leq 1$ for every $i \in J$, and hence representations of matroids are considered as collections of vectors in a vector space.

Let $\mathcal{Z}$ be an integer polymatroid with ground set J. Consider the set $\mathcal{D}$ of the *integer independent vectors of* $\mathcal{Z}$, which is defined as

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

Integer polymatroids can be characterized by its *integer bases*, which are the maximal integer independent vectors. A nonempty subset $\mathcal{B} \subseteq \mathbb{Z}_+^J$ is the family of integer bases of an integer polymatroid if and only if it satisfies the following *exchange condition*.

– For every $u \in \mathcal{B}$ and $v \in \mathcal{B}$ with $u_i > v_i$, there exists $j \in J$ such that $u_j < v_j$ and $u - \mathbf{e}^i + \mathbf{e}^j \in \mathcal{B}$.

In particular, all bases have the same modulus. Every integer polymatroid is univocally determined by the family of its integer bases. Indeed, the rank function of $\mathcal{Z}$ is determined by $h(X) = \max\{|u(X)| \,:\, u \in \mathcal{B}\}$.

Since only integer polymatroids and integer vectors will be considered, we will omit the term "integer" most of the times when dealing with the integer independent vectors or the integer bases of an integer polymatroid.

If $\mathcal{D}$ is the family of independent vectors of an integer polymatroid $\mathcal{Z}$ on J, then, for every $X \subseteq J$, the set $\mathcal{D}|X = \{u(X) \,:\, u \in \mathcal{D}\} \subseteq \mathbb{Z}_+^X$ is the family of independent vectors of an integer polymatroid $\mathcal{Z}|X$ with ground set X. Clearly, the rank function $h|X$ of this polymatroid satisfies $(h|X)(Y) = h(Y)$ for every $Y \subseteq X$. Because of that, we will use the same symbol to denote both rank functions.

For an integer polymatroid $\mathcal{Z}$ and a subset $X \subseteq J$ of the ground set, we write $\mathcal{B}(\mathcal{Z}, X)$ to denote the family of the independent vectors $u \in \mathcal{D}$ such that $\operatorname{supp}(u) \subseteq X$ and $|u| = h(X)$. Observe that there is a natural bijection between $\mathcal{B}(\mathcal{Z}, X)$ and the family of bases of the integer polymatroid $\mathcal{Z}|X$.

2.3 Integer Polymatroids and Multipartite Matroid Ports

The aim of this section is to summarize the results in [12] about ideal multipartite secret sharing schemes and their connection to integer polymatroids.

For a polymatroid $\mathcal{S}$ with ground set $J' = J \cup \{p_0\}$, the family $\Gamma_{p_0}(\mathcal{S}) = \{A \subseteq J \,:\, h(A \cup \{p_0\}) = h(A)\}$ of subsets of J is monotone increasing, and hence it is an access structure on J. If $\mathcal{S}$ is a matroid, then the access structure $\Gamma_{p_0}(\mathcal{S})$ is called the *port of the matroid* $\mathcal{S}$ *at the point* p_0. As a consequence of the results by Brickell [8] and by Brickell and Davenport [9], matroid ports play a very important role in secret sharing. Ports of $\mathbb{K}$-representable matroids are called $\mathbb{K}$-*vector space access structures*. Such an access structure admits an ideal scheme that is constructed according to the method given by Brickell [8]. In addition, Brickell and Davenport [9] proved that the access structure of every ideal secret sharing scheme is a matroid port. This result was generalized in [21] by proving that the access structure of a secret sharing scheme is a matroid port if the length of every share is less than 3/2 times the length of the secret.

Definition 2.1. *Let $\Pi = (\Pi_i)_{i \in J}$ be a partition of a set P of participants. Consider an integer polymatroid $\mathcal{Z}'$ on J' with $h(\{p_0\}) = 1$ and $h(\{i\}) \le |\Pi_i|$ for every $i \in J$, and take $\mathcal{Z} = \mathcal{Z}'|J$. We define a Π-partite access structure $\Gamma_{p_0}(\mathcal{Z}', \Pi)$ in the following way: a vector $u \in \mathbf{P}$ is in $\Gamma_{p_0}(\mathcal{Z}', \Pi)$ if and only if there exist a subset $X \in \Gamma_{p_0}(\mathcal{Z}')$ and a vector $v \in \mathcal{B}(\mathcal{Z}, X)$ such that $v \le u$.*

The following theorem summarizes the results from [12] about the connection between ideal multipartite access structures and integer polymatroids. An access structure is said to be *connected* if all participants are in at least one minimal qualified subset.

Theorem 2.2 ([12]). *Let $\Pi = (\Pi_i)_{i \in J}$ be a partition of a set P. A Π-partite access structure Γ on P is a matroid port if and only if it is of the form $\Gamma_{p_0}(\mathcal{Z}', \Pi)$ for some integer polymatroid $\mathcal{Z}'$ on J' with $h(\{p_0\}) = 1$ and $h(\{i\}) \le |\Pi_i|$ for every $i \in J$. In addition, if $\mathcal{Z}'$ is $\mathbb{K}$-representable, then $\Gamma_{p_0}(\mathcal{Z}', \Pi)$ is an $\mathbb{L}$-vector space access structure for every large enough finite extension $\mathbb{L}$ of $\mathbb{K}$. Moreover, if Γ is connected, the integer polymatroid $\mathcal{Z}'$ is univocally determined by Γ.*

3 Some Useful Integer Polymatroids

In order to find families of ideal multipartite access structures with the required properties, we need to find families of integer polymatroids that are representable over every large enough finite field and can be described in a compact way. To this end, we describe in the following two families of integer polymatroids, namely the Boolean and the uniform ones, and several operations to obtain new polymatroids from some given ones.

3.1 Operations on Polymatroids

We begin by presenting two operations on polymatroids: the sum and the truncation. The first one is a binary operation, while the second one is unitary.

The *sum $\mathcal{Z}_1 + \mathcal{Z}_2$ of two polymatroids* $\mathcal{Z}_1, \mathcal{Z}_2$ on the same ground set J and with rank functions h_1, h_2, respectively, is the polymatroid on J with rank function $h = h_1 + h_2$. If $\mathcal{Z}_1, \mathcal{Z}_2$ are $\mathbb{K}$-representable integer polymatroids, then their sum is $\mathbb{K}$-representable too. Clearly, if $\mathcal{Z}_1$ is represented by the vector subspaces $(V_i)_{i \in J}$ of V and $\mathcal{Z}_2$ is represented by the vector subspaces $(W_i)_{i \in J}$ of W, then the subspaces $(V_i \times W_i)_{i \in J}$ of $V \times W$ form a representation of the sum $\mathcal{Z}_1 + \mathcal{Z}_2$. If $\mathcal{D}_1, \mathcal{D}_2 \subseteq \mathbb{Z}_+^J$ are the sets of independent vectors of $\mathcal{Z}_1$ and $\mathcal{Z}_2$, respectively, then, as a consequence of [28, Theorem 44.6], the independent vectors of $\mathcal{Z}_1 + \mathcal{Z}_2$ are the ones in $\mathcal{D}_1 + \mathcal{D}_2 = \{u_1 + u_2 \,:\, u_1 \in \mathcal{D}_1,\, u_2 \in \mathcal{D}_2\}$. Therefore, the bases of $\mathcal{Z}_1 + \mathcal{Z}_2$ are the vectors in $\mathcal{B}_1 + \mathcal{B}_2$, where $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathbb{Z}_+^J$ are the families of the bases of those polymatroids.

For an integer polymatroid $\mathcal{Z}$ on J with rank function h and a positive integer t with $t \le h(J)$, it is not difficult to prove that the map h' defined by $h'(X) = \min\{h(X), t\}$ is the rank function of an integer polymatroid on J, which is called the *t-truncation of $\mathcal{Z}$*. Observe that a vector $x \in \mathbb{Z}_+^J$ is a basis of the t-truncation of $\mathcal{Z}$ if and only if x is an independent vector of $\mathcal{Z}$ and $|x| = t$.

3.2 Boolean and Uniform Polymatroids

We introduce here two families of integer polymatroids.

The Boolean polymatroids form the first one. They are very simple integer polymatroids that are representable over every finite field. Consider a finite set B and a family $(B_i)_{i \in J}$ of subsets of B. Clearly, the map $h(X) = \left|\bigcup_{i \in X} B_i\right|$ for $X \subseteq J$ is the rank function of an integer polymatroid $\mathcal{Z}$ with ground set J. A *Boolean polymatroid* is an integer polymatroid that can be defined in this way. Boolean polymatroids are representable over every field $\mathbb{K}$. If $|B| = r$, we can assume that B is a basis of the vector space $V = \mathbb{K}^r$. For every $i \in J$, consider the vector subspace $V_i = \langle B_i \rangle$. Obviously, these subspaces form a $\mathbb{K}$-representation of $\mathcal{Z}$. The *modular polymatroids* are those having a *modular rank function*, that is, $h(X \cup Y) + h(X \cap Y) = h(X) + h(Y)$ for every $X, Y \subseteq J$. Every integer modular polymatroid is Boolean, and hence it is representable over every finite field. A Boolean polymatroid is modular if and only if the sets $(B_i)_{i \in J}$ are disjoint. Observe that the rank function of an integer modular polymatroid is of the form $h(X) = \sum_{i \in X} b_i$ for some vector $b \in \mathbb{Z}_+^J$. Actually, this vector is the only basis of such a polymatroid.

Proposition 3.1. *Every truncation of a Boolean polymatroid is representable over every large enough finite field.*

Proof. For a field $\mathbb{K}$ and a positive integer t, we consider the map $\psi_t \colon \mathbb{K} \to \mathbb{K}^t$ defined by $\psi_t(x) = (1, x, \ldots, x^{t-1})$. Observe that, for every t different field elements $x_1, \ldots, x_t \in \mathbb{K}$, the set of vectors $\{\psi_t(x_i) : i = 1, \ldots, t\}$ is linearly independent. Let $\mathcal{Z}$ be a Boolean polymatroid with ground set J, take $r = h(J)$, and consider a field $\mathbb{K}$ with $|\mathbb{K}| \geq r$. Take $B \subseteq \mathbb{K}$ with $|B| = r$ and a family $(B_i)_{i \in J}$ of subsets of B such that $h(X) = \left|\bigcup_{i \in X} B_i\right|$ for every $X \subseteq J$. For a positive integer $t \leq r$ and for every $i \in J$, consider the vector subspace $V_i \subseteq \mathbb{K}^t$ spanned by the vectors in $\{\psi_t(x) : x \in B_i\}$. Clearly, these subspaces form a $\mathbb{K}$-representation of the t-truncation of the Boolean polymatroid $\mathcal{Z}$. □

The second family that is introduced in this section is the one of the uniform polymatroids. We say that a polymatroid $\mathcal{Z}$ with ground set J is *uniform* if every permutation on J is an automorphism of $\mathcal{Z}$. In this situation, the rank $h(X)$ of a set $X \subseteq J$ depends only on its cardinality, that is, there exist values $0 = h_0 \leq h_1 \leq \cdots \leq h_m$, where $m = |J|$, such that $h(X) = h_i$ for every $X \subseteq J$ with $|X| = i$. It is easy to see that such a sequence of values h_i defines a uniform polymatroid if and only if $h_i - h_{i-1} \geq h_{i+1} - h_i$ for every $i \in [1, m-1]$. Clearly, a uniform polymatroid is univocally determined by its *increment vector* $\delta = (\delta_1, \ldots, \delta_m)$, where $\delta_i = h_i - h_{i-1}$. Observe that $\delta \in \mathbb{R}^m$ is the increment vector of a uniform polymatroid if and only if $\delta_1 \geq \cdots \geq \delta_m \geq 0$. A uniform polymatroid is a matroid if and only if $\delta_i \in \{0, 1\}$ for every $i = 1, \ldots, m$. In this case, we obtain the *uniform matroid* $U_{r,m}$, where $r = \max\{i \in [1, m] : \delta_i = 1\}$.

It is well known that $U_{r,m}$ is $\mathbb{K}$-representable whenever $|\mathbb{K}| \geq m$. Obviously, the sum of uniform polymatroids is a uniform polymatroid whose increment vector is obtained by summing up the corresponding increment vectors. The next result was proved in [13].

Proposition 3.2 ([13], Proposition 14). *Every uniform integer polymatroid is a sum of uniform matroids. In particular, every uniform integer polymatroid with ground set J is representable over every field $\mathbb{K}$ with $|\mathbb{K}| \geq |J|$.*

3.3 Multipartite Access Structures from Bases of Integer Polymatroids

We present in the following a consequence of Theorem 2.2 that is very useful in the search of new ideal multipartite access structures. Namely, we prove that a multipartite access structure is ideal if its minimal vectors coincide with the bases of a representable integer polymatroid. We need the following result, which is a consequence of [11, Proposition 2.3].

Proposition 3.3 ([11]). *Let $\mathcal{Z}$ be an integer polymatroid with ground set J and let Λ be an access structure on J. Then there exists an integer polymatroid $\mathcal{Z}'$ on J' with $h(\{p_0\}) = 1$ and $\mathcal{Z} = \mathcal{Z}'|J$ such that $\Lambda = \Gamma_{p_0}(\mathcal{Z}')$ if and only if the following conditions are satisfied.*

1. *If $X \subseteq Y \subseteq J$ and $X \notin \Lambda$ while $Y \in \Lambda$, then $h(X) \leq h(Y) - 1$.*
2. *If $X, Y \in \Lambda$ and $X \cap Y \notin \Lambda$, then $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y) - 1$.*

Proposition 3.4. *Let $\mathcal{Z}$ be a $\mathbb{K}$-representable integer polymatroid on J and let Γ be a Π-partite access structure whose minimal vectors coincide with the bases of $\mathcal{Z}$. Then Γ is an $\mathbb{L}$-vector space access structure for every large enough finite extension $\mathbb{L}$ of $\mathbb{K}$.*

Proof. The access structure $\Lambda = \{X \subseteq J : h(X) = h(J)\}$ and the integer polymatroid $\mathcal{Z}$ satisfy the conditions in Proposition 3.3. Moreover, for this particular access structure, if $\mathcal{Z}$ is $\mathbb{K}$-representable, then the integer polymatroid $\mathcal{Z}'$ whose existence is given by Proposition 3.3 is $\mathbb{L}$-representable for every large enough finite algebraic extension $\mathbb{L}$ of $\mathbb{K}$. Indeed, consider a $\mathbb{K}$-vector space V and vector subspaces $(V_i)_{i \in J}$ forming a $\mathbb{K}$-representation of $\mathcal{Z}$. A representation of $\mathcal{Z}'$ is obtained by finding a vector $v_0 \in V$ such that $v_0 \notin \sum_{i \in X} V_i$ for every $X \subseteq J$ with $h(X) < h(J)$. Since $\sum_{i \in X} V_i \neq V$ if $h(X) < h(J)$, such a vector exists if $\mathbb{K}$ is large enough. Finally, it is not difficult to check that the minimal vectors of $\Gamma_{p_0}(\mathcal{Z}', \Pi)$ coincide with the bases of $\mathcal{Z}$. □

4 Compartmented Access Structures

4.1 Compartmented Access Structures with Upper and Lower Bounds

Simmons [30] introduced compartmented access structures in opposition to the hierarchical ones. Basically, compartmented access structures can be seen as a modification of threshold access structures to be used in situations that require the agreement of several parties. In a compartmented structure, all minimal qualified subsets have the same size, but other requirements are added about the number of participants in every part, or the number of involved parts.

The first examples of compartmented access structures were introduced by Simmons [30]. Brickell [8] introduced a more general family, the so-called *compartmented access structures with lower bounds*, and showed how to construct ideal secret sharing schemes for them. These are the Π-partite access structures defined by $\min \Gamma = \{u \in \mathbf{P} : |u| = t \text{ and } u \geq a\}$ for some vector $a \in \mathbb{Z}_+^J$ and some positive integer t with $t \geq |a|$. The *compartmented access structures with upper bounds* are the Π-partite access structures with $\min \Gamma = \{u \in \mathbf{P} : |u| = t \text{ and } u \leq b\}$, where $b \in \mathbb{Z}_+^J$ and $t \in \mathbb{Z}_+$ are such that $b_i \leq t \leq |b|$ for every $i \in J$. They were introduced by Tassa and Dyn [32], who constructed ideal secret sharing schemes for them.

We introduce in the following a new family of compartmented access structures that generalize the previous ones. Namely, we prove that the compartmented access structures that are defined by imposing both upper and lower bounds on the number of participants in every part are ideal.

For a positive integer t and a pair of vectors $a, b \in \mathbb{Z}_+^J$ with $a \leq b \leq \Pi(P)$, and $|a| \leq t \leq |b|$, and $b_i \leq t$, consider the Π-partite access structure Γ defined by

$$\min \Gamma = \{x \in \mathbf{P} : |x| = t \text{ and } a \leq x \leq b\}. \tag{1}$$

The compartmented access structures with upper bounds and the ones with lower bounds correspond to the compartmented access structures defined above with $a = 0$ and with $b = \Pi(P)$, respectively. We prove in the following that the access structures (1) are ideal by checking that they are of the form $\Gamma_0(\mathcal{Z}', \Pi)$ for a certain family of representable integer polymatroids. Given a positive integer t and two vectors $a, b \in \mathbb{Z}_+^J$ with $a \leq b$ and $|a| \leq t \leq |b|$, consider the vector $c = b - a \in \mathbb{Z}_+^J$ and the integer $s = t - |a| \in \mathbb{Z}_+$. Let $\mathcal{Z}_1$ be the integer modular polymatroid defined by the vector a, and let $\mathcal{Z}_2$ be the s-truncation of the integer modular polymatroid defined by the vector c. Then the integer polymatroid $\mathcal{Z} = \mathcal{Z}_1 + \mathcal{Z}_2$ is representable over every large enough finite field. The family of bases of $\mathcal{Z}$ is $\mathcal{B} = \{x \in \mathbb{Z}_+^J : |x| = t \text{ and } a \leq x \leq b\}$. By Proposition 3.4, this proves that the compartmented access structures of the form (1) are vector space access structures over every large enough finite field.

4.2 Compartmented Compartments

We introduce next another family of compartmented access structures. In this case, instead of an upper bound for every compartment, we have upper bounds for groups of compartments. Take $J = [1, m] \times [1, n]$ and a partition $\Pi = (\Pi_{ij})_{(i,j) \in J}$ of the set P of participants. Take vectors $a \in \mathbb{Z}_+^J$ and $b \in \mathbb{Z}_+^m$, and an integer t with $|a| \leq t \leq |b|$ and $\sum_{j=1}^n a_{ij} \leq b_i \leq t$ for every $i \in [1, m]$.

Consider the Π-partite access structure Γ defined by

$$\min \Gamma = \left\{ x \in \mathbf{P} \,:\, |x| = t, \text{ and } a \leq x, \text{ and } \sum_{j=1}^{n} x_{ij} \leq b_i \text{ for every } i \in [1,m] \right\}.$$

That is, the compartments are distributed into m groups and we have an upper bound for the number of participants in every group of compartments, while we have a lower bound for every compartment.

We prove next that these access structures admit a vector space secret sharing scheme over every large enough finite field. Consider the vector $c \in \mathbb{Z}_+^m$ defined by $c_i = b_i - \sum_{j=1}^{n} a_{ij}$ and the integer $s = t - |a| \in \mathbb{Z}_+$. Let $\mathcal{Z}_1$ be the integer modular polymatroid with ground set J defined by the vector a. Let $\mathcal{Z}_3$ the integer polymatroid with ground set J and family of bases

$$\mathcal{B}_3 = \left\{ x \in \mathbb{Z}_+^J \,:\, \sum_{j=1}^{n} x_{ij} = c_i \text{ for every } i \in [1,m] \right\},$$

and let $\mathcal{Z}_2$ be the s-truncation of $\mathcal{Z}_3$. Finally, take $\mathcal{Z} = \mathcal{Z}_1 + \mathcal{Z}_2$.

Lemma 4.1. *The minimal qualified sets of Γ coincide with the bases of $\mathcal{Z}$.*

Proof. Let $\mathcal{B}$ and $\mathcal{B}_2$ be the families of bases of $\mathcal{Z}$ and $\mathcal{Z}_2$, respectively. The bases of $\mathcal{Z}$ are precisely the vectors of the form $x = a + y$ with $y \in \mathcal{B}_2$. Observe that a vector $y \in \mathbb{Z}_+^J$ is in $\mathcal{B}_2$ if and only if $|y| = s$ and $\sum_{j=1}^{n} y_{ij} \leq c_i$ for every $i \in [1,m]$. □

Lemma 4.2. *The integer polymatroid $\mathcal{Z}$ is representable over every large enough finite field.*

Proof. We only have to prove that this holds for $\mathcal{Z}_2$. By Proposition 3.1, for every large enough finite field $\mathbb{K}$ there exist subspaces $(V_i)_{i\in[1,m]}$ of a $\mathbb{K}$-vector space V that form a representation of the s-truncation of the modular polymatroid with ground set $[1,m]$ defined by the vector c. Then the subspaces $(W_{ij})_{(i,j)\in J}$ of V with $W_{ij} = V_i$ for every $j \in [1,n]$ form a representation of $\mathcal{Z}_2$. □

5 Ideal Partially Hierarchical Access Structures

5.1 Ideal Hierarchical Access Structures

For an access structure Γ on a set P, we say that a participant $p \in P$ is *hierarchically superior in Γ* to a participant $q \in P$, and we write $q \preceq p$, if $A \cup \{p\} \in \Gamma$ for every $A \subseteq P \smallsetminus \{p,q\}$ with $A \cup \{q\} \in \Gamma$. Two participants are *hierarchically equivalent* if $q \preceq p$ and $p \preceq q$. Observe that, if Γ is Π-partite, every pair of participants in the same part Π_i are hierarchically equivalent.

An access structure is *hierarchical* if every pair of participants are hierarchically comparable. In this situation, the hierarchical order $\preceq$ is a total order on

Π. *Weighted threshold access structures*, which were introduced by Shamir [29] in his seminal work, are hierarchical, but they are not ideal in general. The ideal weighted threshold access structures were characterized by Beimel, Tassa and Weinreb [3]. Other examples of hierarchical access structures are the the multilevel access structures introduced by Simmons [30], which were proved to be ideal by Brickell [8], and the hierarchical threshold access structures presented by Tassa [31]. These were the only known families of ideal hierarchical access structures before the connection between integer polymatroids and ideal multipartite secret sharing presented in [12] made it possible to characterize the ideal hierarchical access structures [14]. Actually, all ideal hierarchical access structures are obtained from a special class of Boolean polymatroids [14] and, because of that, they are vector space access structures over every large enough finite field. Moreover, they admit a very compact description, as we see in the following.

Consider two sequences $\mathbf{a} = (a_0, \dots, a_m)$ and $\mathbf{b} = (b_0, \dots, b_m)$ of integer numbers such that $a_0 = a_1 = b_0 = 1$ and $a_i \leq a_{i+1} \leq b_i \leq b_{i+1}$ for every $i \in [0, m-1]$. For $i \in [0, m]$, take the subsets $B_i = [a_i, b_i]$ of the set $B = [1, b_m]$ and consider the Boolean polymatroid $\mathcal{Z}' = \mathcal{Z}'(\mathbf{a}, \mathbf{b})$ with ground set $J' = [0, m]$ defined from them. It is proved in [14] (full version) that a vector $x \in \mathbf{P} \subseteq \mathbb{Z}_+^m$ is in the Π-partite access structure $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$ if and only if there exists $i_0 \in [1, m]$ such that $\sum_{j=1}^{i_0} x_j \geq b_{i_0}$, and $\sum_{j=1}^{i} x_j \geq a_{i+1} - 1$ for all $i \in [1, i_0 - 1]$. Therefore, the participants in Π_i are hierarchically superior to the participants in Π_j if $i \leq j$, and hence every access structure of the form $\Gamma_0(\mathcal{Z}'(\mathbf{a}, \mathbf{b}), \Pi)$ is hierarchical. Moreover, every ideal hierarchical access structure is of this form or it can be obtained from a structure of this form by removing some participants [14].

In particular, if $a_i = 1$ for all $i \in [0, m]$ and $1 = b_0 \leq b_1 < \cdots < b_m$, then $x \in \Gamma_0(\mathcal{Z}'(\mathbf{a}, \mathbf{b}), \Pi)$ if and only if $\sum_{j=1}^{i_0} x_j \geq b_{i_0}$ for some $i_0 \in [1, m]$. These are precisely the *multilevel access structures* introduced by Simmons [30], also called *disjunctive hierarchical threshold access structures* by other authors [31]. They were proved to be ideal by Brickell [8]. On the other hand, the *conjunctive hierarchical threshold access structures* for which Tassa [31] constructs ideal secret sharing schemes are obtained by considering $1 = a_0 = a_1 < \cdots < a_m$ and $1 = b_0 < b_1 = \cdots = b_m$. In this case, $x \in \Gamma_0(\mathcal{Z}'(\mathbf{a}, \mathbf{b}), \Pi)$ if and only if $\sum_{j=1}^{i} x_j \geq a_{i+1} - 1$ for all $i \in [1, m-1]$ and $\sum_{j=1}^{m} x_j \geq b_m$. Observe that, in an access structure in the first family, there may be qualified subsets involving only participants in the lowest level. This is not the case in any access structure in the second family, because every qualified subset must contain participants in the highest level.

By using the results in [14], we can find other ideal hierarchical access structures with more flexible properties. If we take, for instance, $\mathbf{a} = (1, 1, 1, 5, 5)$ and $\mathbf{b} = (1, 4, 6, 10, 12)$, every qualified subset in the hierarchical access structure $\Gamma_0(\mathcal{Z}'(\mathbf{a}, \mathbf{b}), \Pi)$ must contain participants in the first two levels, but some of them do not have any participant in the first level.

5.2 Partial Hierarchies from Boolean Polymatroids

Moreover, by considering other Boolean polymatroids, we can find other families of ideal access structures satisfying some given *partial hierarchy*, that is, Π-partite access structures in which the hierarchical relation $\preceq$ on Π is a partial order. We present next an example of such a family of ideal *partially hierarchical access structures*. Consider a family of subsets $(B_i)_{i \in [0,m]}$ of a finite set B satisfying:

- $|B_0| = 1$ and $B_0 \subseteq B_1$, while $B_0 \cap B_i = \emptyset$ if $i \in [2, m]$, and
- $B_1 \cap B_i \neq \emptyset$ for every $i \in [2, m]$, and
- $B_i \cap B_j = \emptyset$ for every $i, j \in [2, m]$ with $i \neq j$.

Let $\mathcal{Z}'$ be the Boolean polymatroid with ground set $J' = [0, m]$ defined from this family of subsets, and consider the Π-partite access structure $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$. Take $t_1 = |B_1|$ and $t_i = |B_i \smallsetminus B_1|$, and $s_i = |B_i \cap B_1|$ for $i \in [2, m]$. Then a vector $x \in \mathbf{P}$ is in the access structure Γ if and only if there exist a vector $u \in \mathbf{P}$ such that

- $u \leq x$,
- $1 \in \operatorname{supp}(u) = X$, $|u| = \sum_{i \in X} t_i$,
- for every $Y \subseteq X$, $|u(Y)| \leq \sum_{i \in Y} (t_i + s_i)$, where $s_1 = 0$.

Clearly, $q \preceq p$ if $p \in \Pi_1$ and $q \in \Pi_i$ for some $i \in [2, m]$. On the other hand, any two participants in two different parts Π_i, Π_j with $i, j \in [2, m]$ are not hierarchically related.

5.3 Compartmented Access Structures with Hierarchical Compartments

We can consider as well compartmented access structures with hierarchical compartments. Take $J = [1, m] \times [1, n]$ and a partition $\Pi = (\Pi_{ij})_{(i,j) \in J}$ of the set P of participants. Consider a finite set B and a family of subsets $(B_{ij})_{(i,j) \in J}$ such that $B_{in} \subseteq \cdots \subseteq B_{i2} \subseteq B_{i1}$ for every $i \in [1, m]$, and $B_{11} \cup \cdots \cup B_{m1} = B$, and $B_{i1} \cap B_{j1} = \emptyset$ if $i \neq j$. Let $\mathcal{Z}$ be the t-truncation of the Boolean polymatroid defined by this family of subsets. If Γ is a Π-partite access structure such that its minimal vectors coincide with the bases of $\mathcal{Z}$, then Γ is a vector space access structure over every large enough finite field. We now describe Γ. For $(i, j) \in J$, take $b_{ij} = |B_{ij}|$. Consider the vector $b = (b_{11}, \ldots, b_{m1}) \in \mathbb{Z}_+^m$. Of course, $|b| = |B|$. Suppose $b_{i1} \leq t \leq |b|$ for every $i \in [1, m]$. It is not difficult to check that a vector $x \in \mathbb{Z}_+^J$ is a basis of $\mathcal{Z}$, and hence a minimal vector of Γ, if and only if $|x| = t$ and $\sum_{k=j}^{n} x_{ik} \leq b_{ij}$ for every $(i, j) \in J$. Observe that Γ can be seen as a compartmented access structure with compartments $\Pi_i = \bigcup_{j=1}^{n} \Pi_{ij}$ for $i \in [1, m]$, because every minimal qualified subset has exactly t participants, and at most b_{i1} of them in compartment Π_i. In addition, we have a hierarchy within every compartment. Actually, $q \preceq p$ if $p \in \Pi_{ij}$ and $q \in \Pi_{ik}$ with $j \leq k$.

6 Ideal Uniform Multipartite Access Structures

Herranz and Sáez [16, Section 3.2] introduced a family of ideal multipartite access structures that can be seen as a variant of the compartmented ones. Specifically, given integers $1 \le k \le t$, consider the Π-partite access structure defined by

$$\Gamma = \{x \in \mathbf{P} \,:\, |x| \ge t \text{ and } |\operatorname{supp}(x)| \ge k\}. \tag{2}$$

It is proved in [16] that Γ is a vector space access structure over every large enough finite field. Observe that the parts in the partition $\Pi = (\Pi_i)_{i\in J}$ are symmetrical in Γ. That is, the minimal vectors of Γ are invariant under any permutation on J. In the following, we characterize all ideal multipartite access structures with this property. We prove that all of them are vector space access structures over every large enough finite field.

A Π-partite access structure Γ is said to be *uniform* if the set $\min \Gamma \subseteq \mathbb{Z}_+^J$ of its minimal vectors is symmetric, that is, if $u = (u_i)_{i\in J} \in \min \Gamma$, then $\sigma u = (u_{\sigma i})_{i \in J} \in \min \Gamma$ for every permutation σ on J. In this section, we characterize the uniform multipartite access structures that admit an ideal secret sharing scheme. Moreover, we prove that all such access structures are vector space access structures over every large enough finite field. This is done by using the uniform integer polymatroids described in Section 3.2 to construct a family of uniform multipartite access structures that admit a vector space secret sharing scheme over every large enough finite field. Then we prove in Theorem 6.2 that every ideal uniform multipartite access structure is a member of this family.

Let $\mathcal{Z}$ be a uniform integer polymatroid with increment vector δ on a ground set J with $|J| = m$. For $i \in [0, m]$, consider $h_i = \sum_{j=1}^{i} \delta_j$, the values of the rank function of $\mathcal{Z}$. Recall that the (k, m)-threshold access structure on J consists of all subsets of J with at least k elements.

Lemma 6.1. *For an integer $k \in [1, m]$, there exists an integer polymatroid $\mathcal{Z}'_k$ on $J' = J \cup \{p_0\}$ with $h(\{p_0\}) = 1$ and $\mathcal{Z} = \mathcal{Z}'_k|J$ such that $\Gamma_{p_0}(\mathcal{Z}'_k)$ is the (k, m)-threshold access structure on J if and only if $1 \le k \le m - 1$ and $\delta_k > \delta_{k+1}$, or $k = m$ and $\delta_m > 0$.*

Proof. If there exists a polymatroid $\mathcal{Z}'$ with the required properties, then the first condition in Proposition 3.3 implies that $h_{k-1} < h_k$, while $h_{k+1} + h_{k-1} < 2h_k$ if $1 \le k \le m-1$ by the second one. Therefore, our condition is necessary. We prove now sufficiency. Let Λ be the (k, m)-threshold access structure on J. Observe that $h_k > h_{k-1}$ because $\delta_k > 0$, and hence $h(X) < h(Y)$ if $X \subseteq Y \subseteq J$ and $X \notin \Lambda$ while $Y \in \Lambda$. Consider now two subsets $X, Y \in \Lambda$ such that $X \cap Y \notin \Lambda$. This implies in particular that $k < m$. Take $r_1 = |X| \ge k$, $r_2 = |Y| \ge k$, and $s = |X \cap Y| < k$. Then $h_{r_1+r_2-s} - h_{r_2} = \sum_{i=1}^{r_1-s} \delta_{r_2+i} < \sum_{i=1}^{r_1-s} \delta_{s+i} = h_{r_1} - h_s$. The inequality holds because $k = s + i_0$ for some $i_0 \in [1, r_1 - s]$, and hence $\delta_{s+i_0} > \delta_{r_2+i_0}$. Therefore, $h(X \cup Y) + h(X \cap Y) < h(X) + h(Y)$. By Proposition 3.3, this concludes the proof. □

Consider an integer $k \in [1, m]$ in the conditions of Lemma 6.1 and the corresponding integer polymatroid $\mathcal{Z}'_k$. For a partition $\Pi = (\Pi_i)_{i\in J}$ of a set P of participants, consider the Π-partite access structure $\Gamma = \Gamma_{p_0}(\mathcal{Z}'_k, \Pi)$. A vector $v \in \mathbf{P}$ is in Γ if and only if there exists a vector u with $0 \leq u \leq v$ such that

- $s = |\operatorname{supp}(u)| \geq k$ and $|u| = h_s$, and
- $|u(Y)| \leq h_i$ for every $i \in [1, m]$ and for every $Y \subseteq J$ with $|Y| = i$.

As a consequence of the next lemma, $\Gamma = \Gamma_{p_0}(\mathcal{Z}'_k, \Pi)$ is a vector space access structure over every large enough finite field. Moreover, every ideal uniform multipartite access structure is of this form. Due to space limitations, we skip the proof of this result, which will be given in the full version of this paper.

Theorem 6.2. *Let $\Pi = (\Pi_i)_{i \in J}$ with $|J| = m$ be a partition of a set P of participants and let Γ be a uniform Π-partite access structure. Then Γ is ideal if and only if there exist a uniform integer polymatroid $\mathcal{Z}$ on J and an integer $k \in [1, m]$ in the conditions of Lemma 6.1 such that $\Gamma = \Gamma_{p_0}(\mathcal{Z}'_k, \Pi)$. In particular, every ideal uniform multipartite access structure is a vector space access structure over every large enough finite field.*

The uniform multipartite access structures of the form (2) were proved to be ideal in [16]. By using the previous characterization, we obtain a shorter proof for this fact. Consider the uniform integer polymatroid $\mathcal{Z}$ on J with increment vector δ defined by $\delta_1 = t - k + 1$, and $\delta_i = 1$ if $i \in [2, k]$, and $\delta_i = 0$ if $i \in [k+1, m]$. Consider the integer polymatroid $\mathcal{Z}'_k$ whose existence is given by Lemma 6.1. We claim that every Π-partite access structure Γ of the form (2) is equal to $\Gamma(\mathcal{Z}'_k, \Pi)$. Indeed, a vector $v \in \mathbf{P}$ is in $\Gamma(\mathcal{Z}'_k, \Pi)$ if and only if there exists a vector u with $0 \leq u \leq v$ such that

- $s = |\operatorname{supp}(u)| \geq k$ and $|u| = h_s = t$, and
- $|u(Y)| \leq h_i$ for every $i \in [1, m]$ and for every $Y \subseteq J$ with $|Y| = i$.

Since $h_i = t - k + i$ for every $i \in [1, k]$, it is clear that every vector $u \in \mathbf{P}$ satisfying the first condition satisfies as well the second one.

7 Efficiency of the Constructions of Ideal Multipartite Secret Sharing Schemes

Several families of ideal multipartite access structures have been presented in the previous sections. We proved that every one of these structures admits a vector space secret sharing scheme over every large enough finite field. Our proofs are not constructive, but a general method to construct vector space secret sharing schemes for multipartite access structures that are associated to representable integer polymatroids was given in [12]. Unfortunately, this method is not efficient, and no general efficient method is known.

Some issues related to the efficiency of the constructions of ideal schemes for several particular families of multipartite access structures have been considered [8, 5, 15, 31, 32]. We describe in the following a unified framework, derived from the general results in [12], in which those open problems can be more precisely stated.

Take $J = [1, m]$ and $J' = [0, m]$, and let $(\Pi_i)_{i \in J}$ be a partition of the set P of participants, where $|\Pi_i| = n_i$ and $|P| = n$. Consider an integer polymatroid $\mathcal{Z}' = (J', h)$ with $k_i = h(\{i\}) \leq n_i$ for every $i \in J$ and $k_0 = h(\{0\}) = 1$, and take $k = h(J')$. Consider as well a finite field $\mathbb{K}$ and a $\mathbb{K}$-representation $(V_i)_{i \in J'}$ of $\mathcal{Z}'$. In this situation, one has to find a matrix $M = (M_0|M_1|\cdots|M_m)$ over $\mathbb{K}$ with the following properties:

1. M_i is a $k \times n_i$ matrix ($n_0 = 1$) whose columns are vectors in V_i.
2. If $u = (u_0, u_1, \ldots, u_m)$ is a basis of $\mathcal{Z}'$, every $k \times k$ submatrix of M formed by u_i columns in every M_i is nonsingular.

As a consequence of the results in [12], every such a matrix M defines a vector space secret sharing scheme for the multipartite access structure $\Gamma_0(\mathcal{Z}', \Pi)$.

One of the unsolved questions is to determine the minimum size of the fields over which there exists a vector space secret sharing scheme for $\Gamma_0(\mathcal{Z}', \Pi)$. An upper bound can be derived from [12, Corollary 6.7]. Namely, such a matrix M exists if $|\mathbb{K}| > \binom{n+1}{k}$. The best known lower bounds on $|\mathbb{K}|$ are linear on the number of participants, and they can be derived from [1, Lemma 1.2] and other known results about arcs in projective spaces. Even though very large fields are required in general to find such a matrix by using the known methods, the number of bits to represent the elements in the base field is polynomial on the number of participants, and hence the computation of the shares and the the reconstruction of the secret value can be efficiently performed in such a vector space secret sharing scheme.

Another open problem is the existence of efficient methods to construct a vector space secret sharing scheme for $\Gamma = \Gamma_{p_0}(\mathcal{Z}', \Pi)$, that is, the existence of polynomial-time algorithms to compute a matrix M with the properties above. One important drawback is that no efficient method is known to check whether a matrix M satisfying Property 1 satisfies as well Property 2. Moreover, this seems to be related to some problems about representability of matroids that have been proved to be co-NP-hard [26].

We discuss in the following some general construction methods that can be derived from the techniques introduced in previous works [8, 5, 15, 25, 31, 32] for particular families of multipartite access structures.

The first method, which was used in [8, 25] and other works, consists basically in constructing the matrix M column by column, checking at every step that all submatrices that must be nonsingular are so. Arbitrary vectors from the subspaces V_i can be selected at every step, but maybe a wiser procedure is to take vectors of some special form as, for instance, Vandermonde linear combinations of some basis of V_i. In any case, an exponential number of determinants have to be computed.

A probabilistic algorithm was proposed in [31, 32] for multilevel and compartmented access structures. Namely, the vectors from the subspaces V_i are selected at random. This method applies as well to the general case and the success probability is at least $1 - \binom{n+1}{k} N |\mathbb{K}|^{-1}$, where $N = \sum_{i \in J} k_i n_i$. By using this method, a matrix M that, with high probability, defines a secret sharing scheme for the given access structure can be obtained in polynomial time. Nevertheless, no efficient methods to check the validity of the output matrix are known.

Finally, we survey two different methods proposed by Brickell [8] and by Tassa [31] for the hierarchical threshold access structures. Other related solutions appeared in [5, 15] for very particular cases of hierarchical threshold access structures. To better understand these methods, let us consider first the case of the threshold access structures. If the field $|\mathbb{K}|$ is very large, $n+1$ randomly chosen vectors from $\mathbb{K}^k$ will define with high probability an ideal (k, n)-threshold scheme. Nevertheless, no efficient algorithm to check the validity of the output is available. One can instead choose $n+1$ vectors of the Vandermonde form, and in this case an ideal (k, n)-threshold scheme is obtained, and of course we can check its validity in polynomial time. The solutions proposed in those works are based on the same idea. Namely, the vectors from the subspaces V_i have to be of some special form such that a matrix with the required properties is obtained and, in addition, the validity of the output can be efficiently checked. The solution proposed by Brickell [8] is not efficient because it requires to compute a primitive element in an extension field whose extension degree increases with the number of participants. The one proposed by Tassa [31, Section 3.3], which works only for prime fields, provides a polynomial time algorithm to construct a vector space secret sharing scheme for every hierarchical threshold access structure. The existence of similar efficient methods for other families of multipartite access structures is an open problem.

References

1. S. Ball. On large subsets of a finite vector space in which every subset of basis size is a basis. Manuscript (2010), available at the author's webpage.
2. A. Beimel. Secret-Sharing Schemes: A Survey. *IWCC 2011. Lecture Notes in Comput. Sci.* **6639** (2011) 11–46.
3. A. Beimel, T. Tassa, E. Weinreb. Characterizing Ideal Weighted Threshold Secret Sharing. *SIAM J. Discrete Math.* **22** (2008) 360–397.
4. J. Benaloh, J. Leichter. Generalized secret sharing and monotone functions. *Advances in Cryptology, CRYPTO'88. Lecture Notes in Comput. Sci.* **403** (1990) 27–35.
5. A. Beutelspacher, F. Wettl. On 2-level secret sharing. *Des. Codes Cryptogr.* **3** (1993) 127–134.
6. G. R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings.*, **48** (1979) 313–317.
7. J.R. Bloom. A note on Superfast Threshold Schemes. Preprint, Texas A&M. Univ., Dept. of Mathematics, 1981.
8. E. F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.* **9** (1989) 105–113.
9. E. F. Brickell, D. M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology* **4** (1991) 123–134.
10. M.J. Collins. A Note on Ideal Tripartite Access Structures. *Cryptology ePrint Archive*, Report **2002/193**, http://eprint.iacr.org/2002/193.

11. L. Csirmaz. The size of a share must be large. *J. Cryptology* **10** (1997) 223–231.
12. O. Farràs, J. Martí-Farré, C. Padró. Ideal Multipartite Secret Sharing Schemes. *J. Cryptology*, Online First (2011).
13. O. Farràs, J. R. Metcalf-Burton, C. Padró, L. Vázquez. On the Optimization of Bipartite Secret Sharing Schemes. *Des. Codes Cryptogr.*, Online First (2011).
14. O. Farràs, C. Padró. Ideal Hierarchical Secret Sharing Schemes. *Seventh IACR Theory of Cryptography Conference, TCC 2010, Lecture Notes in Comput. Sci.* **5978** (2010) 219–236. The full version of this paper is available at the *Cryptology ePrint Archive*, Report **2009/141**, http://eprint.iacr.org/2009/141.
15. M. Giuletti, R. Vincenti. Three-level secret sharing schemes from the twisted cubic. *Discrete Mathematics* **310** (2010) 3236–3240.
16. J. Herranz, G. Sáez. New Results on Multipartite Access Structures. *IEEE Proceedings on Information Security*, **153** (2006) 153–162.
17. J. Herzog, T. Hibi. Discrete polymatroids. *J. Algebraic Combin.*, **16** (2002) 239–268.
18. M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87.*, (1987) 99–102.
19. E.D. Karnin, J.W. Greene, M.E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory* **29** (1983) 35–41.
20. S.C. Kothari. Generalized Linear Threshold Scheme. *Advances in Cryptology, CRYPTO'84. Lecture Notes in Comput. Sci.* **196** (1985) 231–241.
21. J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *J. Math. Cryptol.* **4** (2010) 95–120.
22. J.L. Massey. Minimal codewords and secret sharing. *Proceedings of the 6-th Joint Swedish-Russian Workshop on Information Theory*, Molle, Sweden, August 1993, pp. 269–279 (1993).
23. S.-L. Ng. Ideal secret sharing schemes with multipartite access structures. *IEEE Proc.-Commun.*, **153** (2006) 165–168.
24. J. G. Oxley, *Matroid theory.* Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.
25. C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory*, **46** (2000) 2596–2604.
26. R. Rao B.V. and J. Sarma M.N. On the Complexity of Matroid Isomorphism Problems. *Computer Science - Theory and Applications, Lecture Notes in Comput. Sci.* **5675** (2009) 286–298.
27. B. Segre. Curve razionali normali e k-archi negli spazi finiti. *Ann. Mat. Pura Appl.* **39** (1955) 357-379.
28. A. Schrijver. *Combinatorial optimization. Polyhedra and efficiency.* Springer-Verlag, Berlin, 2003.
29. A. Shamir. How to share a secret. *Commun. of the ACM*, **22** (1979) pp. 612–613.
30. G. J. Simmons. How to (Really) Share a Secret. *Advances in Cryptology – CRYPTO'88, Lecture Notes in Comput. Sci.*, **403** (1990) 390–448.
31. T. Tassa. Hierarchical Threshold Secret Sharing. *J. Cryptology* **20** (2007) 237–264.
32. T. Tassa, N. Dyn. Multipartite Secret Sharing by Bivariate Interpolation. *J. Cryptology* **22** (2009) 227–258.
33. D. J. A. Welsh. *Matroid Theory.* Academic Press, London, 1976.