SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

July 2015, Vol. 58 072105:1–072105:13
doi: 10.1007/s11432-015-5286-x

Further ideal multipartite access structures from integer polymatroids

WANG YuJue[1,2,3*], WU QianHong[3*], WONG Duncan S.[2],
QIN Bo[4], MU Yi[5] & LIU JianWei[3]

[1]*School of Computer Science, Wuhan University, Wuhan* 430072*, China;*
[2]*Department of Computer Science, City University of Hong Kong, Hong Kong, China;*
[3]*School of Electronics and Information Engineering, Beihang University, Beijing* 100191*, China;*
[4]*School of Information, Renmin University of China, Beijing* 100872*, China;*
[5]*School of Computer Science and Software Engineering, University of Wollongong, Wollongong* NSW2522*, Australia*

Received April 23, 2014; accepted November 26, 2014 ; published online January 30, 2015

Abstract Ideal access structures admit ideal secret sharing schemes where the shares have the minimal size. As multipartite access structures can well mirror the real social organizations, of which the participants are partitioned into disjoint groups according to their properties, it is desirable to find expressive ideal multipartite access structures. Integer polymatroids, due to their close relationship with ideal multipartite access structures, have been shown as a powerful tool to study the ideality of some multipartite access structures. In this paper, to cater for flexible applications, we consider several ideal multipartite access structures that further extend some known results. We first explore a type of compartmented access structures with strictly lower bounds, which provide fairness among all the participant groups when recovering the secret. Then, we investigate ideal bench access structures where the participant set is divided into two parts, that is, line-up section and bench section. The participants in line-up section can delegate their capabilities to the participants in bench section in such a way that the participants in bench section can take over the role of their delegators in line-up section, which is applicable to emergency situations when there are no enough participants in line-up section for recovering the secret. Finally, we propose two types of ideal partially hierarchical access structures which are suitable to more realistic hierarchical social organizations than existing results.

Keywords secret sharing, access structure, multipartite secret sharing, polymatroids, matroids, linear programming

Citation Wang Y J, Wu Q H, Wong D S, et al. Further ideal multipartite access structures from integer polymatroids. Sci China Inf Sci, 2015, 58: 072105(13), doi: 10.1007/s11432-015-5286-x

1 Introduction

Secret sharing [1,2] has been extensively used as an important building block in many cryptographic primitives, for example, distributed (threshold) signature schemes [3], attribute-based signature or encryption schemes [4–6], and group identification schemes [7]. It was originally introduced to guarantee the

* Corresponding author (email: yjwang@whu.edu.cn, qianhong.wu@buaa.edu.cn)

security of storing and accessing secret information. Then, it was proved to be highly related to Reed–Solomon coding [8] and network coding which was widely used for ensuring secure communication [9] and maximizing lifetime [10] of energy-constrained wireless networks.

In a secret sharing scheme, the secret is divided into shares by the dealer and those shares are distributed to the participants in such a way that the secret can be reconstructed by the qualified subsets of participants when pooling their shares together. That is, there is an access policy to recover the secret, which is comparable with the access control policy about how to allow the incoming traffic in the heterogeneous wireless networks [11]. The honest participants follow the scheme faithfully, which is different from that in rational secret sharing schemes [12] where the participants have their own self-interests to recover the secret. Specifically, all the qualified subsets to reconstruct the secret constitute the access structure. In this paper, all the access structures are monotone, that is, every subset of the participants that contains a qualified subset is also qualified.

In the upcoming sections, we only consider perfect secret sharing schemes, that is, every subset in the access structure can reconstruct the secret, while any unqualified subset cannot get any information about the secret. For a perfect secret sharing scheme, the size of each share has to be larger than or equal to the size of the secret [13]. If the length of every share meets lower limit, then the corresponding scheme is ideal [14]. An access structure is ideal if it can be realized by some ideal secret sharing scheme.

The seminal schemes [1,2] were designed for (k, n)-threshold access structures, and thus were called (k, n)-threshold secret sharing schemes. A (k, n)-threshold access structure Γ is of the form $\Gamma = \{A \subseteq P : |A| \geqslant k\}$, that is, after the secret was shared among a set P of n participants, it can be restructured if and only if there are at least k $(1 \leqslant k \leqslant n)$ shares pulling together. For simplicity, due to the monotonicity property of Γ, we can describe it by $\min\Gamma = \{A \subseteq P : |A| = k\}$ which is the family of minimal qualified subsets. It has been shown [15,16] that all the threshold access structures are ideal.

In general, the minimal qualified subsets do not have the same cardinality. According to the results of Ito et al. [17], every access structure admits a linear secret sharing scheme, while in the worst case, the size of the shares may be exponential in n. Benaloh and Leichter [15] and Capocelli et al. [18] proved that for some access structures, for any perfect secret sharing schemes realizing them, the length of some participants' shares have to be larger than the secret. Also, for any positive integer n, Csirmaz [19] constructed an access structure such that for any perfect secret sharing scheme realizing it, the length of some participants' shares must be $O(n/\log n)$ times the length of the secret. In fact, even though some improved results about the upper and lower bounds on the length of the shares have been obtained recently in [20–26], there still exists a gap between the two bounds.

1.1 Multipartite secret sharing

In this section, we review the works on multipartite secret sharing. One can refer to [13,27] for comprehensive survey on secret sharing.

When accessing to a secret, the users in an organization can be usually partitioned into groups and the users of the same group have the same privilege. Multipartite secret sharing is very attractive and supports multipartite access structures over the users in organizations in the real world. An access structure is multipartite if the participant set P can be divided into several disjoint groups such that participants in each group play the same role when reconstructing the secret in the corresponding secret sharing schemes. We proceed to review some well-studied multipartite access structures that are defined on the participant set $P = \cup_{i=1}^{m} P_i$, where P_i's are non-empty, and $P_j \cap P_\ell = \emptyset$ for any distinct $j, \ell \in [1, m]$.

• **Weighted threshold access structures.** In a weighted threshold access structure [2,28,29], each participant is assigned a weight (e.g., according to his/her position in the organization) in such a way that the participants with the same weight belong to the same group and a subset is qualified if and only if the weight sum of its members is greater than some given threshold. A non-ideal weighted threshold scheme can be found in [2] where each participant will receive several shares in proportion to his/her weight. Ideal weighted threshold access structures were well characterized by Beimel, Tassa, and Weinreb [30], and a compact proof was given by Farràs and Padró [31] recently.

• **Compartmented access structures.** The first type of ideal compartmented access structures was introduced by Simmons [32], in which each group (compartment) P_i has a threshold t_i $(1 \leqslant i \leqslant m)$ and the qualified subsets require all the m thresholds are satisfied. Brickell [16] considered a general case where at least $t \geqslant \sum_{i=1}^{m} t_i$ participants are required to reconstruct the secret, which were called compartmented access structure with lower bounds by Tassa and Dyn [33] because the rights of weak compartments can be protected. On the other hand, to restrict the rights of some powerful compartments, compartmented access structures with upper bounds were introduced and also proven to be ideal using bivariate interpolation [33]. These two cases can be unified [34] into compartmented access structures with upper and lower bounds and proven to be ideal based on the relationship between multipartite access structures and integer polymatroids. Farràs et al. [34] also presented another type of ideal compartmented access structures, in which compartments are further divided into some parts, compartmented compartments, such that each compartment has a lower bound and every part of compartments has an upper bound.

• **Uniform multipartite access structures.** Uniform multipartite access structures were first considered by Herranz and Sáez [35], in which every qualified subset comprises at least t participants from no less than k $(1 \leqslant k \leqslant m)$ groups. A compact proof of their ideality was recently given in [34].

• **Uniform threshold access structures.** Simmons [32] introduced another type of ideal compartmented access structures. Compared with the aforementioned compartmented ones, they have different requirements to recover the secret, that is, at least k $(1 \leqslant k \leqslant m)$ thresholds t_i's should be satisfied. For convenience, they are called uniform threshold access structures in the rest of this paper.

• **Quasi-threshold multipartite access structures.** Ng [36] studied a type of ideal quasi-threshold multipartite access structures, in which each group P_i has a threshold t_i $(1 \leqslant i \leqslant m)$, and a special participant p is contained in some group, w.l.o.g., P_1. There are two cases such that the secret can be reconstructed, that is, a set of at least t_1 participants from $P_1 \setminus \{p\}$ is qualified; otherwise, a set contains at least $(t_1 - 1)$ participants from $P_1 \setminus \{p\}$ and no less than k $(1 \leqslant k \leqslant m-1)$ other groups that achieve their thresholds are also qualified. In other words, if the threshold t_1 is not satisfied in the absence of one participant from P_1, then he/she can be substituted by a number of participants in other k groups.

• **Multilevel access structures or hierarchical threshold access structures.** Simmons [32] introduced the first type of multilevel access structures, in which all the participant groups P_i's are pairwise hierarchically comparable and the thresholds satisfy $t_1 \leqslant t_2 \leqslant \cdots \leqslant t_m$. In fact, all the groups form a totally ordered set according to their hierarchies. The qualified subset requires at least one threshold is satisfied, and in the meantime, a participant at a lower level can be replaced by a higher level participant. Brickell [16] proved that these access structures are ideal. They were also called hierarchical threshold access structures with a disjunction of the threshold condition by Tassa [37], which means that the secret can be reconstructed if some threshold is achieved. Its counterpart, hierarchical threshold access structures with a conjunction of the threshold condition, require that all the thresholds have to be fulfilled when reconstructing the secret and were proven ideal using Birkhoff interpolation [37]. Subsequently, Tassa and Dyn [33] further studied them using bivariate interpolation. Recently, ideal hierarchical access structures were well characterized by Farràs and Padró [31]. Some special cases of hierarchical access structures can be found in [38,39]. Note that weighted threshold access structures cannot be covered by the above-mentioned hierarchical threshold ones, and vice versa [37].

• **Partially hierarchical access structures.** Partially hierarchical access structures were introduced by Farràs et al. [34, Section 5] based on the partially ordered set of disjoint groups. Specifically, according to their results, the hierarchical relationships among groups can be seen as a star-like partial order, that is, there exists a higher level group on the center node of a star, and the other groups are placed on the leaf nodes. Also, they considered a type of compartmented access structures with hierarchical compartments, in which the participant groups are further divided into some parts such that the groups in each part constitute a totally ordered set according to their hierarchical relationships.

1.2 Our contributions

This paper focuses on multipartite access structures that admit ideal secret sharing schemes, which can well mirror the practical social organizations to which secret sharing schemes are applied. We

extend several types of compartmented access structures, quasi-threshold access structures, and partially hierarchical access structures and prove that our extensions are ideal in a compact way.

First, we present compartmented access structures with strictly lower bounds and prove their ideality. In a compartmented access structure, the participants of the same group have the equivalent rights when recovering the secret. A compartmented access structures with lower bounds [16,34] can be used to protect the rights of some "weak" groups, which implies that certain level of fairness is guaranteed among different groups of an organization because all thresholds of the groups should be met when reconstructing the secret. However, one or a few groups can still dominate the reconstruction if the quorum to recover the secret is much larger than the sum of the thresholds of all the groups. That is, if $t \gg \sum_{i=1}^{m} t_i$ and $|P_m|$ is large enough, then there may be $(t - \sum_{i=1}^{m-1} t_i)$ participants in P_m taking part in the reconstruction phase, thus the group P_m would perform a more powerful role than the other groups and dominate the reconstructing procedure. To provide better fairness among the groups in reconstructing the secret, we suggest an extra requirement that at least k groups of participants are strictly greater than the lower bounds. In other words, the previous domination is now shared by at least k groups. We show that the extended access structures are still ideal.

Second, we investigate bench (multipartite) access structures. Starting from Ng's [36] quasi-threshold multipartite access structures, we consider a general situation in which the participants are partitioned into two parts, that is, line-up section and bench section. The participants of qualified line-up section can recover the shared secret, but even if all the bench participants pool their shares, they cannot reconstruct the shared secret. The participants in line-up section can delegate their capabilities to the participants in bench section. In case of emergency and some participants of a qualified line-up section are absent, the participants of the bench section can take the role of their absent delegators in line-up section. We show the ideality of bench access structures for both cases that a single participant and multiple participants in line-up section can be substituted. We instantiate bench multipartite access structures, in which the line-up sections are both represented by compartmented access structures with lower bounds, while the bench sections are represented by uniform multipartite ones and uniform threshold ones, respectively.

Finally, we propose more general partially hierarchical access structures. The ideal partially hierarchical access structures introduced by Farràs et al. [34] possess concise partial order, for example, a center connected with leaf nodes. To mirror the general social organizations of participants, we extend the work [34] to two ways. In the first way, each leaf node is replaced by several groups satisfying a totally hierarchical order; and in the second way, each leave node is recursively replaced by a star and the resulting access structure possesses a tree-like hierarchical order. Both extensions are shown to be ideal, which implies that ideal secret sharing is available to hierarchically organized large companies.

2 Preliminaries

2.1 Notations and multipartite access structures

Following [34], we summarize the notations used throughout the paper. Let $\mathbb{Z}_+$ and $\mathbb{R}$ be the non-negative integer set and the real number set, respectively. For i, $j \in \mathbb{Z}_+$, $[i, j]$ denotes the finite integer set from i through j. Given a finite set J and $p_0 \notin J$, $J' \stackrel{\text{def}}{=} J \cup \{p_0\}$. For vectors $\boldsymbol{a} = (a_i)_{i\in J}$ and $\boldsymbol{b} = (b_i)_{i\in J} \in \mathbb{Z}_+^J$, $\boldsymbol{a} \leqslant \boldsymbol{b}$ if and only if $a_i \leqslant b_i$ for every $i \in J$. Furthermore, $\boldsymbol{a} = \boldsymbol{b}$ if and only if both $\boldsymbol{a} \leqslant \boldsymbol{b}$ and $\boldsymbol{a} \geqslant \boldsymbol{b}$ hold. The modulus of a vector $\boldsymbol{a} \in \mathbb{Z}_+^J$ is $|\boldsymbol{a}| \stackrel{\text{def}}{=} \sum_{i\in J} a_i$, which can be easily distinguished from the cardinality $|X|$ of some set X according to the context. The support of $\boldsymbol{a} \in \mathbb{Z}_+^J$ is defined by $\text{supp}(\boldsymbol{a}) \stackrel{\text{def}}{=} \{i \in J : a_i \neq 0\}$. Given a non-empty set $S \subseteq J$ and a vector $\boldsymbol{a} \in \mathbb{Z}_+^J$, $\boldsymbol{a}(S) \stackrel{\text{def}}{=} (a_i)_{i\in S} \in \mathbb{Z}_+^S$. For an access structure Γ on P and two participants p, $q \in P$, $q \preceq p$ represents that p is hierarchically superior to q in Γ, that is, for every $A \subseteq P \setminus \{p, q\}$ such that $A \cup \{q\} \in \Gamma$, we have $A \cup \{p\} \in \Gamma$. Also, if $q \preceq p$ and $p \preceq q$ both hold, then p and q are hierarchically equivalent.

Given a finite set P, let its power set be denoted by $\mathcal{P}(P) = \{A : A \subseteq P\}$ which contains all the subsets of P. If P can be divided into a collection of subsets $\Pi = (\Pi_i)_{i\in J}$ such that $P = \cup_{i\in J}\Pi_i$ and $\Pi_i \cap \Pi_j = \emptyset$ for any two distinct integers i, $j \in J$, then Π is a partition of P. Suppose $\Pi(\cdot)$ is a mapping that is defined from

$\mathcal{P}(P)$ to $\mathbb{Z}_+^J$ such that $\Pi(A) = (|A \cap \Pi_i|)_{i\in J}$, then its range is $\boldsymbol{P} = \Pi(\mathcal{P}(P)) = \{\boldsymbol{a} \in \mathbb{Z}_+^J : \boldsymbol{a} \leqslant (|\Pi_i|)_{i\in J}\}$. For a permutation σ on P, if $\sigma(\Pi_i) = \Pi_i$ holds for every $\Pi_i \in \Pi$, then it is a Π-permutation. Furthermore, since an access structure Γ is a family of subsets of P, that is, $\Gamma \subseteq \mathcal{P}(P)$, if every Π-permutation on Γ is an isomorphism of itself, then Γ is a Π-partite access structure. Clearly, $\Pi(A) \in \Pi(\Gamma) \subseteq \boldsymbol{P}$ for every set $A \in \Gamma$, and $\Pi(\Gamma)$ also satisfies monotonicity property as that in the access structure Γ, that is, for every $\boldsymbol{a} \in \Pi(\Gamma)$ and $\boldsymbol{b} \in \boldsymbol{P}$ such that $\boldsymbol{a} \leqslant \boldsymbol{b}$, we have $\boldsymbol{b} \in \Pi(\Gamma)$. Accordingly, as that of the access structure Γ, $\Pi(\Gamma)$ is also univocally determined by the set $\min \Pi(\Gamma)$ of its minimal vectors.

Definition 1 (Uniform Π-partite access structure [34])**.** For a Π-partite access structure Γ, if the set of its minimal vectors $\min \Gamma \subseteq \mathbb{Z}_+^J$ is symmetric, that is, $\sigma\boldsymbol{a} \in \min \Gamma$ for every minimal vector $\boldsymbol{a} \in \min \Gamma$ and every permutation σ on the set J, then Γ is uniform.

Definition 2 ((Partially) hierarchical access structure [34])**.** For a Π-partite access structure Γ, if the hierarchical relationship $\preceq$ defined on Γ is a total order, then Γ is a hierarchical access structure. Similarly, if $\preceq$ defines a partial order, then Γ is a partially hierarchical access structure.

Clearly, every pair of participants in a hierarchical access structure is hierarchically comparable, and in particular, the participants from the same group are hierarchical equivalent.

2.2 Polymatroids

We briefly review the definitions and some properties with regard to polymatroids [31,34,40,41]. 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, that is, if $X \subseteq Y \subseteq J$, then $h(X) \leqslant h(Y)$;
3. h is submodular, that is, $h(X \cup Y) + h(X \cap Y) \leqslant h(X) + h(Y)$ holds for every $X, Y \subseteq J$.

An integer polymatroid $\mathcal{Z}$ is a polymatroid with an integer-valued rank function h. Suppose $(V_i)_{i\in J}$ are a series of subspaces of a $\mathbb{K}$-vector space V, where $\mathbb{K}$ is a finite field. If there exists a mapping $h(\cdot)$ defined from $\mathcal{P}(J)$ to $\mathbb{Z}$ such that $h(X) = \dim(\sum_{i\in X} V_i)$, then (J, h) determines an integer polymatroid $\mathcal{Z}$, and $\mathcal{Z}$ is said to be $\mathbb{K}$-representable over the vector space V.

For an integer polymatroid $\mathcal{Z}$, the set of integer independent vectors of $\mathcal{Z}$ is $\mathcal{I} \stackrel{\text{def}}{=} \{\boldsymbol{a} \in \mathbb{Z}_+^J : |\boldsymbol{a}(X)| \leqslant h(X)$ for every $X \subseteq J\}$, in which the maximal elements are called the integer bases of $\mathcal{Z}$. Let $\mathcal{B} \subseteq \mathcal{I}$ denote the set of all the integer bases of $\mathcal{Z}$, then all the elements of $\mathcal{B}$ have the identical modulus. In fact, every integer polymatroid $\mathcal{Z}$ is univocally determined by $\mathcal{B}$ because h is determined by $h(X) = \max\{|\boldsymbol{a}(X)| : \boldsymbol{a} \in \mathcal{B}\}$.

Suppose $\mathcal{S}$ is a polymatroid on the ground set $J' = J \cup \{p_0\}$, and let $\Gamma_{p_0}(\mathcal{S}) = \{X \subseteq J : h(X \cup \{p_0\}) = h(X)\}$. It can be seen that $\Gamma_{p_0}(\mathcal{S})$ is an access structure on J because monotonicity property is satisfied. Furthermore, if $\mathcal{S}$ is $\mathbb{K}$-representable and $h(X) \leqslant |X|$ for every subset $X \subseteq J$, then $\Gamma_{p_0}(\mathcal{S})$ is a $\mathbb{K}$-vector space access structure and thus admits an ideal $\mathbb{K}$-vector space secret sharing scheme [42].

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 $\mathcal{B}(\mathcal{Z}, X) = \{\boldsymbol{a} \in \mathcal{I} : \mathrm{supp}(\boldsymbol{a}) \subseteq X$ and $|\boldsymbol{a}| = h(X)\}$ denote a set of integer independent vectors with non-zero coordinates restricted on X.

2.3 Some special integer polymatroids

We describe three special integer polymatroids to be exploited in the paper.

Definition 3 (Boolean polymatroid [34])**.** A Boolean polymatroid is an integer polymatroid $\mathcal{Z} = (J, h)$ such that there exists a collection $(B_i)_{i\in J}$ of subsets of some finite set B and the rank function h can be defined by $h(X) = |\cup_{i\in X} B_i|$ for every subset $X \subseteq J$.

Boolean polymatroids are representable over every finite field, for example, if B is taken as a base of a vector space $V = \mathbb{K}^r$, where $\mathbb{K}$ is some finite field and $r = |B|$, then the corresponding Boolean polymatroid is representable by a collection $(V_i)_{i\in J} = (\langle B_i \rangle)_{i\in J}$ of vector subspaces.

Definition 4 (Modular polymatroid [34]). For a polymatroid $\mathcal{Z} = (J, h)$, if the rank function h is modular, that is, $h(X \cup Y) + h(X \cap Y) = h(X) + h(Y)$ holds for every pair of subsets X, $Y \subseteq J$, then $\mathcal{Z}$ is called a modular polymatroid on the ground set J. Furthermore, if h is integer-valued, then $\mathcal{Z}$ is an integer modular polymatroid.

It can be seen that every integer modular polymatroid is Boolean. Thus, it is also representable over every finite field. However, not all of Boolean polymatroids are modular. In fact, the positive result holds if and only if the corresponding representation sets $(B_i)_{i\in J}$ are disjoint. Note that every integer modular polymatroid $\mathcal{Z} = (J, h)$ has only one base $\boldsymbol{a} \in \mathbb{Z}_+^J$, and the rank function h is defined by $h(X) = |\boldsymbol{a}(X)| = \sum_{i\in X} a_i$.

Definition 5 (Uniform polymatroid [34]). A polymatroid $\mathcal{Z} = (J,\ h)$ is said to be uniform if every permutation σ on J is an automorphism of $\mathcal{Z}$.

It is easy to see that for a uniform polymatroid $\mathcal{Z} = (J, h)$, the rank $h(X)$ is univocally determined by the cardinality $|X|$ of subset $X \subseteq J$. If let $m = |J|$, then there exists a series of values $0 = h_0 \leqslant h_1 \leqslant \cdots \leqslant h_m$ such that $h(X) = h_i$ for every subset $X \subseteq J$ with $|X| = i$. Notate $\delta_i = h_i - h_{i-1}$ for every $i \in [1, m]$. The set $\{h_i\}_{i\in J}$ determines a uniform polymatroid $\mathcal{Z}$ if and only if $\delta_1 \geqslant \cdots \geqslant \delta_m \geqslant 0$. Thus, uniform polymatroid $\mathcal{Z}$ is univocally determined by $\boldsymbol{\delta} = (\delta_1, \ldots, \delta_m)$ which is called an increment vector of $\mathcal{Z}$. Also, every uniform integer polymatroid $\mathcal{Z} = (J, h)$ is representable over every finite field $\mathbb{K}$ with $|\mathbb{K}| \geqslant |J|$.

2.4 Operations on integer polymatroids and access structures

In this paper, we will employ two operations, that is, sum and truncation [34] on integer polymatroids and a composition [31,43] operation on access structures, to explore new useful integer polymatroids and ideal access structures.

Consider two integer polymatroids $\mathcal{Z}_1$ and $\mathcal{Z}_2$ on the same ground set J while with different rank functions h_1, h_2. Their sum is a new integer polymatroid $\mathcal{Z} = (J, h) = \mathcal{Z}_1 + \mathcal{Z}_2$ such that $h = h_1 + h_2$. In particular, if $\mathcal{Z}_1$ and $\mathcal{Z}_2$ are $\mathbb{K}$-representable over vector subspaces $(U_i)_{i\in J}$ of U and $(V_i)_{i\in J}$ of V, respectively, then $\mathcal{Z} = \mathcal{Z}_1 + \mathcal{Z}_2$ is $\mathbb{K}$-representable over vector subspaces $(U_i \times V_i)_{i\in J}$ of $U \times V$. According to the results of [34], the set of integer bases of $\mathcal{Z}$ is $\mathcal{B} = \mathcal{B}_1 + \mathcal{B}_2 = \{\boldsymbol{a} + \boldsymbol{b} : \boldsymbol{a} \in \mathcal{B}_1 \ and \ \boldsymbol{b} \in \mathcal{B}_2\}$, where $\mathcal{B}_1$, $\mathcal{B}_2 \subseteq \mathbb{Z}_+^J$ represent the sets of integer bases of $\mathcal{Z}_1$ and $\mathcal{Z}_2$, respectively.

Given an integer polymatroid $\mathcal{Z} = (J, h)$. For any positive integer $t \leqslant h(J)$, the t-truncation $\mathcal{Z}'$ of $\mathcal{Z}$ is defined by a pair of (J, h'), where the rank function h' satisfies $h'(X) = \min\{h(X), t\}$. Also, the set of integer bases of $\mathcal{Z}'$ is $\mathcal{B}' = \{\boldsymbol{a} \in \mathcal{B} : |\boldsymbol{a}| = t\}$, where $\mathcal{B} \subseteq \mathbb{Z}_+^J$ is the set of integer bases of $\mathcal{Z}$.

An access structure Γ on P is connected if and only if there exist no redundant participants in it, that is, every participant belongs to some minimal qualified subset. Suppose Γ_1, Γ_2 are two connected access structures on disjoint sets P_1 and P_2, respectively. For any $p \in P_1$, the composition of Γ_1 and Γ_2 over p is defined as an access structure $\Gamma = \Gamma_1[\Gamma_2; p]$ on the set $P = P_1 \cup P_2$, that is,

$$\Gamma = \Gamma_1[\Gamma_2; p] = \left\{ A \subseteq P : \begin{array}{l} A \cap P_1 \in \Gamma_1, \text{ or} \\ (A \cup \{p\}) \cap P_1 \in \Gamma_1 \text{ and } A \cap P_2 \in \Gamma_2 \end{array} \right\}.$$

It has been shown [43] that for two $\mathbb{K}$-vector space access structures, their composition is also $\mathbb{K}$-representable over some vector space.

2.5 Ideal multipartite access structures and integer polymatroids

There is a close relationship between ideal multipartite access structures and integer polymatroids [40], which plays an important role to find some new ideal access structures [34]. In this paper, integer polymatroids are further shown to be a powerful tool to search new ideal access structures and give compact proofs for the ideality.

Lemma 1 ([34]). Consider a partition $\Pi = (\Pi_i)_{i\in J}$ of a set P. If an integer polymatroid $\mathcal{Z}' = (J', h)$ satisfies $h(\{p_0\}) = 1$ and $h(\{i\}) \leqslant |\Pi_i|$ for every $i \in J$, then

$$\Gamma = \Gamma_{p_0}(\mathcal{Z}', \Pi) = \{\boldsymbol{a} \in \mathcal{P}(P) : \exists X \in \Gamma_{p_0}(\mathcal{Z}') \text{ and } \boldsymbol{b} \in \mathcal{B}(\mathcal{Z}'|J, X) \text{ such that } \boldsymbol{b} \leqslant \boldsymbol{a}\}$$

defines a Π-partite access structure on P. Also, 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 $\mathbb{K}$; and if Γ is connected on P, then it univocally determines the existence of $\mathcal{Z}'$.

In fact, to prove the ideality of a multipartite access structure, it suffices to check whether the minimal vectors of the access structure coincide with the bases of some representable integer polymatroids [34].

3 Compartmented access structures with strictly lower bounds

Compartmented access structures with lower bounds $\Gamma = \{\boldsymbol{x} \in \boldsymbol{P} : |\boldsymbol{x}| \geqslant t \text{ and } \boldsymbol{x} \geqslant \boldsymbol{a}\}$ were first considered by Brickell [16], where the corresponding vector space secret sharing schemes were realized using the linear-algebraic method. In a different way, Tassa and Dyn [33] designed ideal secret sharing schemes for them using bivariate Lagrange interpolation with data on parallel lines. In [34], a compact proof on their ideality was given by Farràs et al. according to the relationship between ideal multipartite access structures and integer modular polymatroids.

Compartmented access structures with lower bounds, as noted by Tassa and Dyn [33], can ensure the fairness among all the groups to a certain degree in reconstruction of the secret, because the involved participants pooling their shares together must come from all the groups such that all the thresholds a_i $(1 \leqslant i \leqslant m)$ are met. However, the reconstruction can still be dominated by one or a few groups even when the basic agreement reached among all groups. For example, if $t \gg \sum_{i=1}^{m} a_i$ and all the groups are large enough, then for a qualified subset $(a_1, \ldots, a_{m-1}, t - \sum_{i=1}^{m-1} a_i)$, in which all of $(t - \sum_{i=1}^{m} a_i)$ additional participants belong to the group P_m, the secret could be recovered even if the participants in other groups just meet their thresholds. Thus, to some extent the group P_m of a large population dominates the reconstructing procedure.

A similar problem occurs in compartmented access structures with upper and lower bounds $\min\Gamma = \{\boldsymbol{x} \in \boldsymbol{P} : |\boldsymbol{x}| = t \text{ and } \boldsymbol{a} \leqslant \boldsymbol{x} \leqslant \boldsymbol{b}\}$. For instance, if $t \gg \sum_{i=1}^{m} a_i$ but $t - \sum_{i=1}^{m-2} a_i \leqslant b_{m-1} + b_m$, and all the groups are large enough, then for every qualified subset like $(a_1, \ldots, a_{m-2}, b_{m-1}, t - \sum_{i=1}^{m-2} a_i - b_{m-1})$, the groups P_{m-1} and P_m have dominance over the reconstruction.

We address the above problem using ideal compartmented access structures with strictly lower bounds. Not only the number of participants in every group has a lower bound, but also at least k groups of participants are required to be strictly greater than the lower bounds, when their shares are pooled together to reconstruct the secret. In such a way, the domination of some groups occurring in previous discussion will be shared by at least k groups. Therefore, this type of access structures can provide better fairness among groups than compartmented access structures with lower bounds.

Definition 6 (Compartmented access structures with strictly lower bounds). Given some integer vector $\boldsymbol{a} \in \mathbb{Z}_+^J$, let Π be an m-partition of the participant set P, where $m = |J|$, and t and k be two positive integers that satisfy $t \geqslant |\boldsymbol{a}|$ and $1 \leqslant k \leqslant \min\{m, t - |\boldsymbol{a}|\}$, respectively. A type of compartmented access structures with strictly lower bounds are defined by the following Π-partite access structures:

$$\min\Gamma = \{\boldsymbol{x} \in \boldsymbol{P} : |\boldsymbol{x}| = t, \text{ and } \boldsymbol{x} \geqslant \boldsymbol{a}, \text{ and } |\mathrm{supp}(\boldsymbol{x} - \boldsymbol{a})| \geqslant k\}. \tag{1}$$

Theorem 1. Π-partite access structure (1) is ideal.

Proof. Let $\mathcal{Z}_1$ be an integer modular polymatroid that is defined by the vector $\boldsymbol{a}$. Thus, it is representable over every large enough finite field. Then, we consider uniform Π-partite access structure Γ':

$$\min\Gamma' = \{\boldsymbol{x} \in \boldsymbol{P'} : |\boldsymbol{x}| = t - |\boldsymbol{a}| \text{ and } |\mathrm{supp}(\boldsymbol{x})| \geqslant k\}, \tag{2}$$

where $\boldsymbol{P'} = \{\boldsymbol{y} \in \mathbb{Z}_+^J : \boldsymbol{y} \leqslant (|\Pi_i| - a_i)_{i\in J}\}$.

In [34, Section 6], Farràs et al. proved that Γ' is ideal by showing that there exists an uniform integer polymatroid $\mathcal{Z}_2$ on the ground set J and an integer $k \in [1, m]$ such that $\Gamma' = \Gamma_{p_0}(\mathcal{Z}'_k, \Pi)$, where $\mathcal{Z}'_k$ is an integer polymatroid on the ground set $J' = J \cup \{p_0\}$ with $h(\{p_0\}) = 1$ and $\mathcal{Z}_2 = \mathcal{Z}'_k|J$ and $\Gamma_{p_0}(\mathcal{Z}'_k)$ is a (k, m)-threshold access structure on set J. Specifically, the rank function h of $\mathcal{Z}_2$ is defined by the increment vector

$$\boldsymbol{\delta} = (t - |\boldsymbol{a}| - k + 1, \underbrace{1, 1, \ldots, 1, 1}_{\text{coordinates } 2,\ldots,k}, \underbrace{0, 0, \cdots, 0, 0}_{\text{coordinates } k+1,\ldots,m}).$$

That is, $h_i = t - |\boldsymbol{a}| - k + i$ for every $i \in [1, k]$ and $h_i = h_k$ for every $i \in [k + 1, m]$. As a consequence of the results in [34], Γ' admits a vector space secret sharing scheme over every large enough finite field, that is, it is ideal.

Thus, $\mathcal{Z} = \mathcal{Z}_1 + \mathcal{Z}_2$ is representable over every large enough finite field and the set of its bases is

$$\mathcal{B} = \{\boldsymbol{x} \in \mathbb{Z}_+^J : |\boldsymbol{x}| = t,\ \boldsymbol{x} \geqslant \boldsymbol{a},\ |\mathrm{supp}(\boldsymbol{x} - \boldsymbol{a})| \geqslant k\}.$$

By Lemma 1, we know that Π-partite access structure (1) is ideal.

4 Ideal bench access structures

We consider a situation in which the participant set is partitioned into line-up section and bench section. The participants in line-up section can recover the secret when pooling their shares together according to the corresponding access structure, while the secret cannot be recovered even if all the participants of bench section pool their shares together. A participant or several participants jointly can delegate their capabilities to a subaccess structure on the bench section. In this way, if these participants are absent such that there are no enough participants in line-up section to meet the minimum requirements for recovering the secret, then the absent participants can be substituted by a number of participants in bench section. Clearly, the bench access structures we considered here differ from standard multilevel (or hierarchical threshold) access structures, because in the latter, the participants in lower level groups are unable to substitute high-level ones when the secret cannot be recovered.

Our bench access structures provide a remedy mechanism for accessing to sensitive information in the case of emergency. In general, the participants in bench section will not be involved into the reconstruction algorithm; while in some emergency situation where no enough participants in line-up section can achieve the minimal qualified requirements, the participants in bench section can take part in the reconstruction algorithm on behalf of their delegators. We first prove a type of bench access structures are ideal, where each delegator participant in line-up section can separately designate a subaccess structure on the bench section. We also discuss the case in which more than one participant in line-up section can be jointly substituted. Then, we give two special instances, that is, bench multipartite access structures, in both of which, the qualified line-up section is represented by compartmented access structures with lower bounds, while the bench section qualified for substitution is represented by uniform multipartite access structures and uniform threshold ones, respectively. Note that the second instance of bench multipartite access structures is more general than Ng's quasi-threshold multipartite access structures [36].

Theorem 2. For a bench access structure where some participant in line-up section delegates his/her capability to a number of participants in bench section, if both the line-up section and the bench section can be modelled by ideal access structures, then this bench access structure is also ideal.

Proof. Consider a bench access structure Γ on the participant set P, of which the line-up section Γ' and bench section Γ'' are defined on the sets of P' and P'', respectively. Note that $P' \cup P'' = P$ and $P' \cap P'' = \emptyset$. According to the definition of the bench access structures, the secret can be recovered by any qualified subset in Γ', and if the delegator participant $p \in P'$ is absent with regard to Γ', a lot of participants in P'' can take the role of p. Thus, Γ can be composed of Γ' and Γ'' over p, that is, $\Gamma = \Gamma'[\Gamma''; p]$. By taking into account the fact that the composition of two ideal access structures is also an ideal access structure [43], we complete the proof.

We proceed to consider the case such that more than one participant in a minimal qualified subset in line-up section can be substituted by the participants in the bench section. Following Martí-Farré et al. [43], we use $\Gamma = \Gamma' \sqcup \Gamma''$ to denote the disjoint union of Γ' and Γ'', where Γ' and Γ'' are two connected access structures on the disjoint sets P' and P'', respectively. Thus, Γ is on the participant set $P = P' \cup P''$ and $\min\Gamma = \min\Gamma' \cup \min\Gamma''$. An access structure Γ is said to be strongly connected if it cannot be denoted as the disjoint union of other access structures. In fact, every connected access structure Γ can be represented as a r-disjoint union $\Gamma = \Gamma_1 \sqcup \cdots \sqcup \Gamma_r$ for some integer r, where all the Γ_i's are strongly connected.

Theorem 3. For a bench access structure where r participants in line-up section jointly delegate their capabilities to a number of participants in bench section, if both the line-up section and the bench section can be modelled by ideal access structure and ideal r-disjoint union access structure, respectively, then this bench access structure is also ideal.

Proof. Consider a bench access structure Γ on the participant set P, of which the line-up section Γ' and bench section Γ'' are defined on the sets of P' and P'', respectively. Note that $P' \cup P'' = P$ and $P' \cap P'' = \emptyset$. Since Γ'' is a r-disjoint union access structure, that is, $\Gamma'' = \Gamma_1 \sqcup \cdots \sqcup \Gamma_r$, Γ'' is ideal if all the Γ_i's are ideal [43]. As Γ can be seen as the composition of the line-up section with r Γ_i's step by step, according to the previous theorem, all the intermediate compositions and the final result Γ are all ideal if Γ' and all the Γ_i's are ideal.

Note that those r participants in line-up section should be unqualified to recover the secret, otherwise, the participants in bench section are also able to recover it. In fact, r participants in line-up section can also be substituted by an ideal γ-disjoint union access structure such that $\gamma < r$.

Following [40], a matroid is a special integer polymatroid $\mathcal{Q} = (J,\ h)$ such that $h(Y) \leqslant |Y|$ for every $Y \subseteq J$. Then, for a non-empty subset $Y \subset J$, we can define an access structure on $J \setminus Y$ as $\Gamma_Y(\mathcal{Q}) = \{X \subseteq J \setminus Y : h(X \cup Y) = h(X)\}$.

Lemma 2. Given two matroids $\mathcal{Q}_1$ and $\mathcal{Q}_2$ on the ground sets J_1 and J_2, respectively, where $J_1 \cap J_2 = Y$ and $|Y| \geqslant 1$. Consider $\Gamma_1 = \Gamma_p(\mathcal{Q}_1)$, where $p \in J_1 \setminus Y$, and $\Gamma_2 = \Gamma_Y(\mathcal{Q}_2)$. The composition of Γ_1 and Γ_2 over Y is defined as an access structure $\Gamma = \Gamma_1[\Gamma_2; Y]$ on the set $P = J_1 \cup J_2 \setminus \{p\}$, that is,

$$\Gamma = \Gamma_1[\Gamma_2; Y] = \left\{ A \subseteq P : \begin{array}{l} A \cap (J_1 \setminus \{p\}) \in \Gamma_1, \text{ or} \\ (A \cup Y) \cap (J_1 \setminus \{p\}) \in \Gamma_1 \text{ and } A \cap (J_2 \setminus Y) \in \Gamma_2 \end{array} \right\}.$$

The access structure Γ is $\mathbb{K}$-representable over some vector space if and only if both Γ_1 and Γ_2 are $\mathbb{K}$-vector space access structures.

The proof is similar to that of [44, Proposition 7.1.21] and [43, Proposition 2.1 and 2.2]. Furthermore, we have the following results.

Theorem 4. For a bench access structure Γ where an unqualified set Y of participants in line-up section jointly delegate their capabilities to a number of participants in bench section, if both the line-up section and the bench section can be modelled by ideal access structures Γ_1 and Γ_2 as shown in Lemma 2, respectively, then this bench access structure is also ideal.

4.1 Bench section with uniform multipartite access structures

Let Π be an m-partition of the participant set P, where $m = |J|$, $S \subsetneq J$ be a non-empty subset, and t and k are two positive integers that satisfy $1 \leqslant k \leqslant \min\{m - |S|, t\}$. Given some integer vector $\boldsymbol{a} \in \mathbb{Z}_+^S$, consider a Π-partite access structure Γ, in which the line-up section is a compartmented access structure with lower bounds Γ' defined on $|S|$ disjoint groups, that is, $\min\Gamma' = \{\boldsymbol{x} \in \boldsymbol{P'} : \boldsymbol{x} = \boldsymbol{a}\}$, where $\boldsymbol{P'} = \{\boldsymbol{y}(S) : \forall \boldsymbol{y} \in \boldsymbol{P}\}$; and the bench section is an uniform multipartite access structure on $(m - |S|)$ disjoint groups, that is, $\min\Gamma'' = \{\boldsymbol{x} \in \boldsymbol{P''} : |\boldsymbol{x}| = t \text{ and } |\mathrm{supp}(\boldsymbol{x})| \geqslant k\}$, where $\boldsymbol{P''} = \{\boldsymbol{y}(J \setminus S) : \forall \boldsymbol{y} \in \boldsymbol{P}\}$. Suppose a participant p of a subset in $\min\Gamma'$ has delegated his capability to the participants in Γ''. Thus, any element in Γ'' can substitute for p when recovering the secret, and Γ is a composition of Γ' and Γ''

over p, that is,

$$\Gamma = \Gamma'[\Gamma''; p] = \left\{ \boldsymbol{x} \in \boldsymbol{P} : \begin{array}{l} \boldsymbol{x}(S) \geqslant \boldsymbol{a}, \text{ or} \\ \left\{ \begin{array}{l} x_i = a_i - 1 \text{ for some } i \in S, \text{ and} \\ \boldsymbol{x}(S \setminus \{i\}) \geqslant \boldsymbol{a}(S \setminus \{i\}), \text{ and} \\ |\boldsymbol{x}(J \setminus S)| \geqslant t, \text{ and} \\ |\mathrm{supp}(\boldsymbol{x}(J \setminus S))| \geqslant k \end{array} \right. \end{array} \right\}.$$

Note that both Γ' and Γ'' are ideal [34]. Thus Γ is an ideal access structure.

4.2 Bench section with uniform threshold access structures

Consider some integer vector $\boldsymbol{a} \in \mathbb{Z}_+^J$. Let Π be an m-partition of the participant set P, where $m = |J|$, $S \subsetneq J$ be a non-empty subset, and t and k be two positive integers that satisfy $1 \leqslant k \leqslant m - |S|$. Consider a Π-partite access structure Γ, in which the line-up section is a compartmented access structure with lower bounds Γ' defined on $|S|$ disjoint groups, that is, $\min \Gamma' = \{\boldsymbol{x} \in \boldsymbol{P'} : \boldsymbol{x} = \boldsymbol{a}(S)\}$, where $\boldsymbol{P'} = \{\boldsymbol{y}(S) : \forall \boldsymbol{y} \in \boldsymbol{P}\}$; and the bench section is an uniform threshold access structure on $(m - |S|)$ disjoint groups, that is,

$$\Gamma'' = \bigcup_{S' \subseteq J \setminus S, |S'| = k} \{\boldsymbol{x} \in \boldsymbol{P''} : x_i \geqslant a_i \text{ for every } i \in S'\},$$

where $\boldsymbol{P''} = \{\boldsymbol{y}(J \setminus S) : \forall \boldsymbol{y} \in \boldsymbol{P}\}$. Suppose a participant p of a subset in $\min \Gamma'$ has delegated his capability to the participants in Γ''. Thus, any element in Γ'' can substitute for p when recovering the secret, and Γ is a composition of Γ' and Γ'' over p, that is,

$$\Gamma = \Gamma'[\Gamma''; p] = \left\{ \boldsymbol{x} \in \boldsymbol{P} : \begin{array}{l} \boldsymbol{x}(S) \geqslant \boldsymbol{a}(S), \text{ or} \\ \left\{ \begin{array}{l} x_i = a_i - 1 \text{ for some } i \in S, \text{ and} \\ \boldsymbol{x}(S \setminus \{i\}) \geqslant \boldsymbol{a}(S \setminus \{i\}), \text{ and} \\ \boldsymbol{x}(S') \geqslant \boldsymbol{a}(S') \text{ for some } S' \subseteq J \setminus S \text{ such that } |S'| \geqslant k \end{array} \right. \end{array} \right\}.$$

Due to the facts that both Γ' and Γ'' are ideal access structures [32,34], it follows that Γ is ideal as well. Note that in [36], a special case of this type of Π-partite access structures Γ, that is, $S = \{1\}$, has been proven ideal.

5 Ideal partially hierarchical access structures

In real-world applications, the secrets are always shared among hierarchically organized companies. Thus, it is desirable to find the corresponding ideal access structures that can well mirror the companies' social structures. We proceed to show the existence of ideal partially hierarchical access structures which are suitable for such applications. Our starting point is a type of partially hierarchical access structures due to Farràs et al. [34, Section 5].

5.1 Partially hierarchical access structures with totally ordered hierarchical compartments

In the partially hierarchical access structures [34], the corresponding Boolean polymatroid is representable by the subsets $(B_i)_{i \in [0,m]}$ of a finite set B such that they satisfy some predefined conditions. The relationship among these subsets $(B_i)_{i \in [0,m]}$ can be depicted by a "star-like graph," where the set B_1 is placed at the center and the other sets B_i $(i \in [2, m])$ are the leaves. In the following generalization, we show that if each "leaf node" is replaced by a hierarchical compartment such that the participant groups within every hierarchical compartment constitute a totally ordered set, then the resulting access structure is still ideal.

Consider a family of subsets B_0, B_1, and $(B_{ij})_{(i,j) \in [2,m] \times [1,n]}$ of a finite set B such that:

1. $B_0 \subseteq B_1$ and $|B_0| = 1$, but $B_0 \cap B_{ij} = \emptyset$ for every $(i, j) \in [2, m] \times [1, n]$;

2. $B_1 \cap B_{i1} \neq \emptyset$ for every $i \in [2, m]$;

3. $B_{i1} \cap B_{j1} = \emptyset$ for every i, $j \in [2, m]$ with $i \neq j$;

4. $B_{in} \subseteq \cdots \subseteq B_{i2} \subseteq B_{i1}$ for every $i \in [2, m]$.

Let $\mathcal{Z}'$ be a Boolean polymatroid on the ground set $J' = \{0, 1\} \cup [2, m] \times [1, n]$, which was defined by the above subsets B_0, B_1, and $(B_{ij})_{(i,j)\in[2,m]\times[1,n]}$. It is easy to find an ideal Π-partite access structure $\Gamma = \Gamma_0(\mathcal{Z}', \Pi)$ such that its minimal qualified sets coincide with the bases of $\mathcal{Z}'$ due to the fact that the Boolean polymatroids are representable over every finite field. Clearly, the participants in the group corresponding to B_1 have the highest hierarchy and all the participants in the same compartment are hierarchically comparable, while the participants from different compartments are hierarchically unrelated.

Although the above extension looks similar to the second family of compartmented access structures with hierarchical compartments presented in [34, Subsection 5.3], they are different in the following aspects:

1. Each qualified subset in our case for recovering the secret must contain at least $|B_1|$ participants in the participant group corresponding to B_1, while this was not required (or the special case $B_1 = \emptyset$) in [34, Subsection 5.3].

2. For every compartment in our case, if it has some participants being contained in some minimum qualified subset, then this subset requires at least $|B_{i1} \setminus B_1|$ ($i \in [2, m]$) participants from this compartment.

3. Disjoint subsets $(B_{i1})_{i\in[1,m]}$ of B satisfy $B_{11} \cup \cdots \cup B_{m1} = B_1$ and $B_{i1} \cap B_{j1} = \emptyset$ if $i \neq j$ in [34, Subsection 5.3], while the requirements on the similar subsets are more relaxed in our case.

5.2 Tree-like partially hierarchical access structures

For the second type of compartmented access structures with hierarchical compartments introduced by Farràs et al. [34, Subsection 5.3], each node of the star-like graph is replaced by a path. When mirroring this scenario of sharing a secret among a company, it implies that each department of the company has a single direct subordinate department. One may observe that the companies are usually organized in tree-like structures. This motivates us to extend Farràs et al.'s work to partially hierarchical access structures with tree-like hierarchical structures. Encouragingly, this type of access structures are still ideal, which implies that there exist ideal secret sharing schemes according to the participants' social privileges in large-scale institutions with complicated organizations.

Let $J = [1, m]$ and $\Pi = (\Pi_i)_{i\in J}$ be a partition of the participant set P. Consider a family of subsets $(B_i)_{i\in[1,m]}$ of a finite set B. We view B as the root of a tree and $(B_i)_{i\in[1,m]}$ as intermediate nodes or leaves according to their hierarchical positions. Specifically, these subsets satisfy:

1. for the root B, if its children are denoted by $B_1, B_2, \ldots, B_\ell$, then $B_1 \cup \cdots \cup B_\ell = B$ and $B_i \cap B_j = \emptyset$ for every $i \neq j$ and i, $j \in [1, \ell]$;

2. for every non-leaf node B_i, if its children are denoted by $B_{i_1}, \ldots, B_{i_h}$, then $B_{i_1} \cup \cdots \cup B_{i_h} \subseteq B_i$ and $B_{i_j} \cap B_{i_k} = \emptyset$ for every $j \neq k$ (j, $k \in [1, h]$).

Let $\mathcal{Z}$ be the t-truncation of a Boolean polymatroid which is defined by subsets $(B_i)_{i\in J}$, where $\max\{|B_i|\} \leqslant t \leqslant |B|$. It is also easy to find an ideal Π-partite access structure Γ such that its minimal qualified sets coincide with the bases of $\mathcal{Z}$ due to the fact that the truncation of a Boolean polymatroid is representable over every finite field [34]. In fact, if the root B has ℓ children $B_1, \ldots, B_\ell$, then Γ has ℓ compartments Π'_i ($i \in [1, \ell]$). Furthermore, for each B_i ($i \in [1, \ell]$) together with all of its descendants B_j's, their corresponding groups (Π_i and Π_j's) of participants constitute the compartment Π'_i.

The hierarchical relationships between the participants are also simple. On one hand, for every subset B_i and its descendant B_j, the corresponding groups are denoted by Π_i and Π_j, respectively. Then, $p \succeq q$ holds for any $p \in \Pi_i$ and $q \in \Pi_j$. On the other side, for any subsets B_i and B_j which do not satisfy the relationship like "ancestor" and "descendant," the participants from the corresponding groups Π_i and Π_j are hierarchically unrelated.

6 Conclusion

We extended several ideal multipartite access structures to support flexible applications. The extended compartmented access structures with strictly lower bounds would be more effective in protecting fairness among all groups of participants than existing compartmented ones. The proposed ideal bench access structures provide a useful remedy mechanism in case of emergency to reconstruct the secret when some participants are absent in the reconstruction procedure. The generalized ideal partially hierarchical access structures are useful to share a secret among the companies with complicated organizational structures.

It remains open to design effective vector space secret sharing schemes for generally multipartite access structures. Among a lot of methods proposed in recent years, only a few algorithms with regard to some special types of multipartite access structures are efficient. Prominent works include Tassa's polynomial time algorithm with regard to hierarchical threshold access structures [37]. A general method has been considered for multipartite access structures associated with representable integer polymatroids in [40], albeit it is not efficient.

Acknowledgements

The authors are supported by National Key Basic Research Program of China (973 Program) (Grant No. 2012CB315905), National Natural Science Foundation of China (Grant Nos. 61370190, 61173154, 61472429, 61402029, 61272501, 61202465), and Beijing Natural Science Foundation (Grant Nos. 4132056, 4122041). We thank Dr. Oriol Farràs for helpful discussions and many insightful comments that greatly improve the paper.

References

1 Blakley G R. Safeguarding cryptographic keys. In: Proceedings of the 1979 AFIPS National Computer Conference, Monval, 1979. 313–317
2 Shamir A. How to share a secret. Commun ACM, 1979, 22: 612–613
3 Wang Y J, Wong D S, Wu Q H, et al. Practical distributed signatures in the standard model. In: Proceedings of the Cryptographer's Track at the RSA Conference, San Francisco, 2014. 307–326
4 Deng H, Wu Q H, Qin B, et al. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Inform Sci, 2014, 275: 370–384
5 Deng H, Wu Q H, Qin B, et al. Who is touching my cloud. In: Proceedings of the 19th European Symposium on Research in Computer Security, Part I, Wroclaw, 2014. 362–379
6 Liu W R, Liu J W, Wu Q H, et al. Practical direct chosen ciphertext secure key-policy attribute-based encryption with public ciphertext test. In: Proceedings of the 19th European Symposium on Research in Computer Security, Part II, Wroclaw, 2014. 91–108
7 Tang C M, Gao S H. Leakproof secret sharing protocols with applications to group identification scheme. Sci China Inf Sci, 2012, 55: 1172–1185
8 McEliece R J, Sarwate D V. On sharing secrets and Reed-Solomon codes. Commun ACM, 1981, 24: 583–584
9 Feldman J, Malkin T, Servedio R A, et al. Secure network coding via filtered secret sharing. In: Proceedings of 42nd Annual Allerton Conference on Communication, Control, and Computing, Illinois, 2004. 30–39
10 Ding L H, Wu P, Wang H, et al. Lifetime maximization routing with network coding in wireless multihop networks. Sci China Inf Sci, 2013, 56: 022303
11 Zheng J, Li J D, Liu Q, et al. Performance analysis of three multi-radio access control policies in heterogeneous wireless networks. Sci China Inf Sci, 2013, 56: 122305
12 Zhang Z F, Liu M L. Rational secret sharing as extensive games. Sci China Inf Sci, 2013, 56: 032107
13 Beimel A. Secret-sharing schemes: a survey. In: Proceedings of the 3rd International Workshop on Coding and Cryptology, Qingdao, 2011. 11–46
14 Karnin E D, Greene J W, Hellman M E. On secret sharing systems. IEEE Trans Inform Theory, 1983, 29: 35–41
15 Benaloh J, Leichter J. Generalized secret sharing and monotone functions. In: Proceedings of Advances in Cryptology—CRYPTO'88, Santa Barbara, 1988. 27–35
16 Brickell E F. Some ideal secret sharing schemes. In: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, Houthalen, 1989. 468–475
17 Ito M, Saito A, Nishizeki T. Secret sharing scheme realizing general access structure. In: IEEE/IEICE Global Telecommunications Conference, Tokyo, 1987. 99–102
18 Capocelli R M, de Santis A, Gargano L, et al. On the size of shares of secret sharing schemes. J Cryptol, 1993, 6:

157–168
19 Csirmaz L. The size of a share must be large. J Cryptol, 1997, 10: 223–231
20 Farràs O, Metcalf-Burton J R, Padró C, et al. On the optimization of bipartite secret sharing schemes. Des Codes Cryptogr, 2012, 63: 255–271
21 Martí-Farré J, Padró C. On secret sharing schemes, matroids and polymatroids. J Math Cryptol, 2010, 4: 95–120
22 Padró C, Sáez G. Secret sharing schemes with bipartite access structure. IEEE Trans Inform Theory, 2000, 46: 2596–2604
23 Padró C, Vázquez L, Yang A. Finding lower bounds on the complexity of secret sharing schemes by linear programming. Discrete Appl Math, 2013, 161: 1072–1084
24 Beimel A, Livne N. On matroids and non-ideal secret sharing. IEEE Trans Inform Theory, 2008, 54: 482–501
25 Beimel A, Livne N, Padró C. Matroids can be far from ideal secret sharing. In: Proceedings of the 5th Conference on Theory of Cryptography, New York, 2008. 194–212
26 Beimel A, Orlov I. Secret sharing and non-shannon information inequalities. IEEE Trans Inform Theory, 2011, 57: 539–557
27 Stinson D R. An explication of secret sharing schemes. Des Codes Cryptogr, 1992, 2: 357–390
28 Beimel A, Weinreb E. Monotone circuits for monotone weighted threshold functions. Inf Process Lett, 2006, 97: 12–18
29 Morillo P, Padró C, Sáez G, et al. Weighted threshold secret sharing schemes. Inf Process Lett, 1999, 70: 211–216
30 Beimel A, Tassa T, Weinreb E. Characterizing ideal weighted threshold secret sharing. SIAM J Discrete Math, 2008, 22: 360–397
31 Farràs O, Padró C. Ideal hierarchical secret sharing schemes. IEEE Trans Inform Theory, 2012, 58: 3273–3286
32 Simmons G J. How to (really) share a secret. In: Proceedings of Advances in Cryptology—CRYPTO'88, Santa Barbara, 1988. 390–448
33 Tassa T, Dyn N. Multipartite secret sharing by bivariate interpolation. J Cryptol, 2009, 22: 227–258
34 Farràs O, Padró C, Xing C, et al. Natural generalizations of threshold secret sharing. IEEE Trans Inform Theory, 2014, 60: 1652–1664
35 Herranz J, Sáez G. New results on multipartite access structures. IEE Proc Inf Secur, 2006, 153: 153–162
36 Ng S L. Ideal secret sharing schemes with multipartite access structures. IEE Proc Commun, 2006, 153: 165–168
37 Tassa T. Hierarchical threshold secret sharing. J Cryptol, 2007, 20: 237–264
38 Beutelspacher A, Wettl F. On 2-level secret sharing. Des Codes Cryptogr, 1993, 3: 127–134
39 Giuletti M, Vincenti R. Three-level secret sharing schemes from the twisted cubic. Discrete Math, 2010, 310: 3236–3240
40 Farràs O, Martí-Farré J, Padró C. Ideal multipartite secret sharing schemes. J Cryptol, 2012, 25: 434–463
41 Herzog J, Hibi T. Discrete polymatroids. J Algebr Comb, 2002, 16: 239–268
42 Brickell E F, Davenport D M. On the classification of ideal secret sharing schemes. J Cryptol, 1991, 4: 123–134
43 Martí-Farré J, Padró C. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. Des Codes Cryptogr, 2009, 52: 1–14
44 Oxley J G. Matroid Theory. New York: Oxford University Press, 1992. 238–270