Wireless Pers Commun (2015) 82:283–292
DOI 10.1007/s11277-014-2208-y

New Results on Ideal Multipartite Secret Sharing and its Applications to Group Communications

Ching-Fang Hsu · Shan Wu · Lein Harn

Published online: 30 November 2014

Abstract With the rapid development of various group-oriented services, multipartite group communications occur frequently in a single network, where a multipartite access structure is defined to be a collection of the subsets of users who may come from different parts of the network such that only users in an authorized subset of users can use their shares to build up a group key for a secure group communication. Most existing group key establishment schemes based on a secret sharing target on building up a group key for a threshold access structure, and need to compute a t-degree interpolating polynomial in order to encrypt and decrypt the secret group key. This approach is not suitable and inefficient in terms of computational complexity for multipartite group environments which need to realize the multipartite access structures. In 1991, Brickell et al. proved that an ideal access structure is induced by a matroid and furthermore, an access structure is ideal if it is induced by a representable matroid. In this paper, we study the characterization of representable matroids. By using the connection between ideal secret sharing and matroids and, in particular, the recent results on ideal multipartite access structures and the connection between multipartite matroids and discrete polymatroids, we introduce a new concept on R-tuple, which is determined by the rank function of the associated discrete polymatroid. Using this new concept, we come up a new and simple sufficient condition for a multipartite matroid to be representable (in fact, every matroid and every access structure are multipartite). In other words, we have developed a sufficient condition for an access structure to be ideal. These new results can be applied to establish multipartite group keys efficiently in secure group communications.

This work was supported by the Nature Science Foundation of China (No. 61100221, 61003192).

C.-F. Hsu
Computer School, Central China Normal University, Wuhan 430079, China

S. Wu (✉)
Wuhan Technology and Business University, Wuhan 430065, China
e-mail: cherryjingfang@gmail.com

L. Harn
Department of Computer Science Electrical Engineering, University of Missouri,
Kansas City, MO 64110, USA

Keywords Group communications · Ideal multipartite secret sharing · Ideal access structures · Representable multipartite matroids · Discrete polymatroids

1 Introduction

Group communication means a type of many-to-many communication. It can go beyond a one-to-one communication (i.e., unicast) and a one-to-many communication (i.e., multicast). The privacy of a group communication is usually ensured using a symmetric encryption key. All members in a group share a secret session (group) key. The group key establishment problem has been studied extensively in the literatures [1,2]. In most solutions, conventional encryption and decryption operations are needed to distribute group keys [3–6]. Secret sharing scheme which was first introduced by Blakley [7] and Shamir [8] in 1979 has been used to design group key establishment protocols [9–12]. Using secret sharing scheme can avoid the use of one-to one encryption and thus reduce the computational complexity. Furthermore, the security of using a secret sharing scheme is unconditionally secure which is much preferable than conditionally secure using any conventional encryption. Secret sharing has been used to design group key establishment protocols [9–12]. Laih et al. [13] proposed the first algorithm using a (t, n) secret sharing scheme to distribute a group key to group members. Later, there are papers [14–16] following the same approach to propose ways to distribute group messages to users. Recently, [17] proposed a novel group key transfer protocol using secret sharing which can provide confidentiality and authentication.

With the rapid development of various group-oriented services, multipartite group communications occur frequently in a single network, where a multipartite access structure is defined to be a collection of the subsets of users who may come from different parts of the network such that only users in an authorized subset of users can use their shares to build up a group key for a group communication. In a multipartite group communication, group keys establishment requests of a multipartite access structure are mostly serviced by a service provider. For example, let us assume in an IEEE 802.16 network [18], a service provider provides three different services, e.g., a charged TV streaming service, a telematics service, and an information service. In this example, there exists three user parts such that users in the same part play equivalent role in the access structure. Each part of users should be managed according to a multipartite access structure defined by the service provider such that users in an authorized subset can use their shares to build up a group key for a secure group communication. Most group key establishment schemes based on a secret sharing target on building up a group key for a threshold access structure. It needs to compute a t-degree interpolating polynomial in order to encrypt and decrypt the secret group key. It is obvious that this approach is not suitable and inefficient interms of computational complexity for multipartite group environments which need to realize multipartite access structures.

A secret sharing scheme for a access structure Γ is a method in which a dealer distributes shares of a secret to participants such that (1) any subset in Γ can reconstruct the secret from its shares, and (2) any subset not in Γ cannot obtain any partial information about the secret in the information theoretic sense. A secret sharing scheme is called *ideal* if shares of shareholders are taken from the same domain as the secret. As proved in [19], the size of shares in an ideal secret sharing has the optimal size which is the same size of the secret. In addition, the access structures which can be realized by ideal secret sharing schemes are called *ideal access structures*. Thus, we are motivated by exploring the possibility to develop ideal multipartite secret sharing schemes and use them use these schemes to design efficient and secure multipartite group keys establishment protocols.

Multipartite access structure, informally, is a set of participants which can be divided into several parts such that participants in the same part play equivalent role in the structure. Since we can consider the situation that the number of parts is the same as the number of participants, every access structure is multipartite (in this way, every matroid is multipartite). Secret sharing for multipartite access structures has been studied by several authors. The group keys establishment using a threshold secret sharing is the most straightforward approach. For example, schemes use a secret sharing scheme to construct group keys establishment for a threshold access structure (i.e., a unipartite access structures) which is the simplest multipartite access structure.

Multipartite access structures were first introduced by Shamir [8] in his seminal work, in which weighted threshold access structures were considered. Beimel, Tassa and Weinreb [20] presented a characterization of the ideal weighted threshold access structures that generalizes the partial results in [21,22]. A complete characterization of the ideal bipartite access structures was given in [22], and related results were given independently in [23,24]. Partial results on the characterization of the ideal tripartite access structures appeared in [25,26], and this question was solved in [27]. Another important result about a complete characterization of the ideal hierarchical access structures has been obtained by Farras and Padro [28]. They proved that every ideal hierarchical access structure is induced by a representable matroid. This connection of polymatroids and the associated access structures have been studied in [29]: Recently, by using the reduced discrete polymatroids, [30] obtained a sufficient condition for a multipartite access structure to be ideal and further give a new proof that all access structures related to bipartite and tripartite matroids coincide with the ideal ones. All these families of multipartite access structures described above are related to representable matroids, and hence, they are the ideal ones.

In 1991, Brickell and Davenport [31] proved that an ideal access structure is induced by a matroid. Furthermore, an access structure is ideal if it is induced by a representable matroid. In this paper, we study the characterization of representable matroids. By using the connection between ideal secret sharing and matroids and, in particular, the recent results on ideal multipartite access structures and the connection between multipartite matroids and discrete polymatroids, we introduce a new concept on R-tuple, which is determined by the rank function of the associated discrete polymatroid. Furthermore, we propose a new and simple sufficient condition for a multipartite matroid which is representable. This sufficient condition is a general result (i.e., every matroid and every access structure are multipartite). Further, we use an unipartite and a bipartite group communications as two examples to explain this sufficient condition. These new results are interesting for developing efficient and secure multipartite-group-oriented solutions.

2 Definitions and Preliminaries

In this section we review some basic definitions and notations [19,25] that will be used through the paper.

2.1 Secret Sharing Schemes

Let $P = \{p_i : 1 \leq i \leq n\}$ be a set of participants. The dealer is denoted by D and we assume $D \notin P$. $\mathcal{K}$ is the secret set (i.e. the set of all possible secrets) and $\mathcal{S}$ is the share set (i.e. the set of all shares). Let Γ be a collection of the subsets of P: this is denoted mathematically by the notation $\Gamma \subseteq 2^P$. The subsets in Γ are those subsets of participants that are able to reconstruct the secret. Γ is called an access structure and the subsets in Γ are called authorized subsets. Accordingly, $\Delta = 2^P \backslash \Gamma$ is called a prohibited structure and the subsets in Δ are called unauthorized subsets.

When the dealer D wants to share a secret $K \in \mathcal{K}$, he will give each participant a share from $\mathcal{S}$. The shares should be distributed secretly. At a later time, a subset of participants will attempt to reconstruct K from the shares collectively hold. Using Shannon's entropy function, we will say that a scheme is a perfect secret sharing scheme realizing the access structure Γ satisfies the following two properties:

1. **Validity:** $H(K \mid A) = 0, \forall A \in \Gamma$ (Any authorized subset of participants $A \in \Gamma$ who pool their shares together can reconstruct the secret K),
2. **Security:** $H(K \mid A) = H(K), \forall A \in \Delta$ (Any unauthorized subset of participants $A \in \Delta$ who pool their shares together obtain no information on K).

2.2 Multipartite Access Structures

We write $\mathcal{P}(P)$ as the power set of the set P. An m-partition $\Pi = \{P_1, \ldots, P_m\}$ of a set P is a disjoint family of m nonempty subsets of P with $P = P_1 \cup \ldots \cup P_m$. Let $\Lambda \subseteq \mathcal{P}(P)$ be a family of subsets of P. For a permutation σ on P, we define $\sigma(\Lambda) = \{\sigma(A) : A \in \Lambda\} \subseteq \mathcal{P}(P)$. A family of subsets $\Lambda \subseteq \mathcal{P}(P)$ is said to be Π-partite if $\sigma(\Lambda) = \Lambda$ for every permutation σ such that $\sigma(P_i) = P_i$ for every $P_i \in \Pi$. We say that Λ is m-partite if it is Π-partite for some m-partition Π. These concepts can be applied to access structures, which are actually families of subsets, and they can be applied as well to the family of independent sets of a matroid. A matroid $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ is Π-partite if $\mathcal{I} \subseteq \mathcal{P}(\mathcal{Q})$ is Π-partite.

Let $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ be a connected matroid and, for a point $p_0 \in \mathcal{Q}$, let $\Pi = \{P_1, \ldots, P_m\}$ and $\Pi_0 = \{\{p_0\}, P_1, \ldots, P_m\}$ be partitions of the sets $P = \mathcal{Q} - \{p_0\}$ and $\mathcal{Q}$ respectively. Then the access structure $\Gamma = \Gamma_{p_0}(\mathcal{M})$ is Π-partite if and only if the matroid $\mathcal{M}$ is Π_0-partite.

For every integer $m \geq 1$, we consider the set $J_m = \{1, \ldots, m\}$. Let $\mathbb{Z}_+^m$ denote the set of vectors $u = (u_1, \ldots, u_m) \in \mathbb{Z}^m$ with $u_i \geq 0$ for every $i \in J_m$. For a partition $\Pi = \{P_1, \ldots, P_m\}$ of a set P and for every $A \subseteq P$ and $i \in J_m$, we define $\Pi_i(A) = |A \cap P_i|$. Then the partition Π defines a mapping $\Pi : \mathcal{P}(P) \to \mathbb{Z}_+^m$ by considering $\Pi(A) = (\Pi_1(A), \ldots, \Pi_m(A))$. If $\Lambda \subseteq \mathcal{P}(P)$ is Π-partite, then $A \in \Lambda$ if and only if $\Pi(A) \in \Pi(\Lambda)$. That is, Λ is completely determined by the partition Π and the set of vectors $\Pi(\Lambda) \subset \mathbb{Z}_+^m$.

Discrete polymatroids, a combinatorial object introduced by Herzog and Hibi [32], are closely related to multipartite matroids and, because of that, they play an important role in the characterization of ideal multipartite access structures. Before giving the definition of discrete polymatroid, we need to introduce some notation. If $u, v \in \mathbb{Z}_+^m$, we write $u \leq v$ if $u_i \leq v_i$ for every $i \in J_m$, and we write $u < v$ if $u \leq v$ and $u \neq v$. The vector $w = u \vee v$ is defined by $w_i = \max(u_i, v_i)$. The modulus of a vector $u \in \mathbb{Z}_+^m$ is $|u| = u_1 + \cdots + u_m$. For every subset $X \subseteq J_m$, we write $u(X) = (u_i)_{i \in X} \in \mathbb{Z}_+^{|X|}$ and $|u(X)| = \sum_{i \in X} u_i$.

A discrete polymatroid on the ground set J_m is a nonempty finite set of vectors $D \subset \mathbb{Z}_+^m$ satisfying:

1. if $u \in D$ and $v \in \mathbb{Z}_+^m$ is such that $v \leq u$, then $v \in D$, and
2. for every pair of vectors $u, v \in D$ with $|u| < |v|$, there exists $w \in D$ with $u < w \leq u \vee v$.

The next proposition, which is easily proved from the axioms of the independent sets of a matroid, shows the relation between multipartite matroids and discrete polymatroids.

Proposition 2.1 *Let Π be a partition of a set $\mathcal{Q}$ and let $\mathcal{I} \subseteq \mathcal{P}(\mathcal{Q})$ be a Π-partite family of subsets. Then $\mathcal{I}$ is the family of the independent sets of a Π-partite matroid $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ if and only if $\Pi(\mathcal{I}) \subset \mathbb{Z}_+^m$ is a discrete polymatroid.*

A basis of a discrete polymatroid D is a maximal element in D, that is, a vector $u \in D$ such that there does not exist any $v \in D$ with $u < v$. Similarly to matroids, a discrete polymatroid is determined by its bases. Specifically, the following result is proved in [32, Theorem 2.3].

Proposition 2.2 *A nonempty subset $\mathcal{B} \subset \mathbb{Z}_+^m$ is the family of bases of a discrete polymatroid if and only if it satisfies:*

1. *all elements in $\mathcal{B}$ have the same modulus, and*
2. *for every $u \in \mathcal{B}$ and $v \in \mathcal{B}$ with $u_i > v_i$, there exists $j \in J_m$ such that $u_j < v_j$ and $u - e_i + e_j \in \mathcal{B}$, where e_i denotes the i-th vector of the canonical basis of $\mathbb{Z}^m$.*

The rank function of a discrete polymatroid D with ground set J_m is the function $h : \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = \max\{|u(X)| : u \in D\}$. The next proposition is a consequence of [32, Theorem 3.4].

Proposition 2.3 *A function $h : \mathcal{P}(J_m) \to \mathbb{Z}$ is the rank function of a discrete polymatroid with ground set J_m if and only if it satisfies*

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

Moreover, a polymatroid D is completely determined by its rank function. Specifically, $D = \left\{u \in \mathbb{Z}_+^m : |u(X)| \leq h(X) \text{ for all } X \subseteq J_m\right\}$.

Let $\mathbb{K}$ be a field, E a $\mathbb{K}$-vector space, and $V_1, \ldots, V_m$ subspaces of E. It is not difficult to check that the mapping $h : \mathcal{P}(J_m) \to \mathbb{Z}$ defined by $h(X) = \dim(\sum_{i \in X} V_i)$ is the rank function of a discrete polymatroid $D \subset \mathbb{Z}_+^m$. In this situation, we say that D is $\mathbb{K}$-representable and the subspaces $V_1, \ldots, V_m$ are a $\mathbb{K}$-representation of D. The next proposition is proved in [27, Theorem 7.1].

Proposition 2.4 *Let $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ be a Π-partite matroid and let $D = \Pi(\mathcal{I})$ be its associated discrete polymatroid. If $\mathcal{M}$ is $\mathbb{K}$-representable, then so is D. In addition, if D is $\mathbb{K}$-representable, then $\mathcal{M}$ is representable over some finite extension of $\mathbb{K}$.*

3 Operations on Discrete Polymatroids

In this section, by dealing with the rank function of a discrete polymatroid, we introduce the definition on the R-tuple of a discrete polymatroid, which is very useful for the following result in this paper.

Let D be a discrete polymatroid with ground set J_m and rank function $h : \mathcal{P}(J_m) \to \mathbb{Z}$. For any $i, j, k \in J_m$, we write $\mathcal{P}(J_m - \{j\})$, $\mathcal{P}(J_m - \{j, k\})$ and $\mathcal{P}(J_m)$ for the power sets of $J_m - \{j\}$, $J_m - \{j, k\}$ and J_m respectively, and we firstly define the following denotations (since they are all calculated by the rank function of D and hence, we denote them by the first letter of "rank") that will be used through the paper.

Denotations:

1. $r(i \cap j) = h(\{i\}) + h(\{j\}) - h(\{i, j\})$,
   $r(i \cap j \cap k) = h(\{i\}) + h(\{j\}) + h(\{k\}) - h(\{i, j\}) - h(\{i, k\}) - h(\{j, k\}) + h(\{i, j, k\})$,
   $\ldots, r\left(\bigcap_{i \in J_m} i\right) = \sum_{i \in J_m} h(\{i\}) - \sum_{i,j \in J_m} h(\{i, j\}) + \ldots + (-1)^{|J_m|-1} h(J_m)$, and

2. $\Delta r(i) = h(J_m) - h(J_m - \{i\})$,
   $\Delta r(i \cap j) = h(J_m) - h(J_m - \{i, j\}) - \Delta r(i) - \Delta r(j)$
   $= h(J_m - \{i\}) + h(J_m - \{j\}) - h(J_m - \{i, j\}) - h(J_m), \ldots,$
   $\Delta r\left(\bigcap_{i \in J_m - \{j\}} i\right) = h(J_m) - h(\{j\}) - \sum_{A \in \mathcal{P}(J_m - \{j\}) - \{J_m - \{j\}\}} \Delta r\left(\bigcap_{k \in A} k\right),$
   $r\left(\bigcap_{i \in J_m} i\right) = h(J_m) - \sum_{A \in \mathcal{P}(J_m) - \{J_m\}} \Delta r\left(\bigcap_{j \in A} j\right).$

   In this situation, it is not difficult to check that

$$h(\{j\}) = r\left(\bigcap_{i \in J_m} i\right) + \sum_{A \in \mathcal{P}(J_m) - \{J_m\} - \mathcal{P}(J_m - \{j\})} \Delta r\left(\bigcap_{k \in A} k\right), \tag{1}$$

$$h(\{j, k\}) = r\left(\bigcap_{i \in J_m} i\right) + \sum_{A \in \mathcal{P}(J_m) - \{J_m\} - \mathcal{P}(J_m - \{j,k\})} \Delta r\left(\bigcap_{l \in A} l\right), \tag{2}$$

$$\ldots, h(J_m) = r\left(\bigcap_{i \in J_m} i\right) + \sum_{A \in \mathcal{P}(J_m) - \{J_m\}} \Delta r\left(\bigcap_{j \in A} j\right). \tag{3}$$

Next we give the definition on the R-tuple of a discrete polymatroid.

Definition 3.1 Let $D \subset \mathbb{Z}_+^m$ be a discrete polymatroid with ground set J_m and rank function $h : \mathcal{P}(J_m) \to \mathbb{Z}$. For all $i, j, k \in J_m$, by the known rank function of D, we compute C_m^1 values of $\Delta r(i), C_m^2$ values of $\Delta r(i \cap j), C_m^3$ values of $\Delta r(i \cap j \cap k)$,..., C_m^{m-1} values of $\Delta r(\bigcap_{i \in J_m - \{j\}} i)$ and C_m^m value of $r(\bigcap_{i \in J_m} i)$. There are altogether $t = C_m^1 + C_m^2 + \ldots + C_m^m$ values. We say that $R = \{\Delta r(i), \Delta r(i \cap j), \ldots, \Delta r(\bigcap_{i \in J_m - \{j\}} i), r(\bigcap_{i \in J_m} i) :$ for all $i, j, k \in J_m\}$ is the R-tuple of D, where $|R| = t$.

4 A New Sufficient Condition for a Multipartite Matroid to be Representable

In this section, by using the R-tuple of the associated discrete polymatroid, a new sufficient condition for a multipartite matroid to be representable is present, which is fairly interesting for determining ideal access structures related to representable matroids.

The main goal of this section is to prove the following result:

Theorem 4.1 *Let $D \subset \mathbb{Z}_+^m$ be a discrete polymatroid with ground set J_m and rank function $h : \mathcal{P}(J_m) \to \mathbb{Z}$. If the R-tuple of D is nonnegative, that is, all elements of the R-tuple of D are all nonnegative integers, then D is representable over some finite field.*

Proof Let $s = h(J_m)$ and $E = \mathbb{K}^s$ be a s-dimensional vector space over some finite field $\mathbb{K}$ with $|\mathbb{K}| \geq s$. Given a basis $\{v_1, \ldots, v_s\}$ of E, consider the mapping $\mathbf{v} : \mathbb{K} \to E$ defined by $\mathbf{v}(x) = \sum_{i=1}^{s} x^{i-1} v_i$. Observe that the vectors $\mathbf{v}(x)$ have Vandermonde coordinates with respect to the given basis of E. This implies that every set of at most s vectors of the form $\mathbf{v}(x)$ is independent (this property is very important to the following proof). □

Consider t disjoint sets $S_1, \ldots, S_t \subseteq \{\mathbf{v}(x) : x \in \mathbb{K}\} \subset E$ with $|S_i| = R_i (1 \leq i \leq t)$, where R_i is the i–th entry of the R-tuple. Observe that $\sum_{i=1}^{t} |S_i| = s$ according to (3). This implies that all s vectors in $S_1, \ldots, S_t$ are independent.

According to (1), we construct m subspaces $V_1, \ldots, V_m \subseteq E$ such that for every $j \in J_m, V_j$ is spanned by $\bigcup_{\sum |S_i| = h(\{j\})} S_i$ respectively. In this situation, according to (1) (2) (3), we obtain that for all $A \subseteq J_m$, the dimensions $\dim(\sum_{j \in A} V_j) = h(A)$. Therefore, m subspaces $V_1, \ldots, V_m$ of the vector space $E = \mathbb{K}^s$ is a $\mathbb{K}$-representation of D. Therefore, D is representable over $\mathbb{K}$.

As a consequence, from Proposition 2.4, Theorem 4.1 provides a new sufficient condition for a multipartite matroid to be representable.

The further importance of Theorem 4.1 is that it provides a sufficient condition for a multipartite access structure to be ideal. Namely, a multipartite access structure is ideal if it is of the form $\Gamma_{p_0}(\mathcal{M})$, where $\mathcal{M} = (\mathcal{Q}, \mathcal{I})$ is a Π-partite matroid and $\Pi(\mathcal{I})$ is the corresponding discrete polymatroid D such that the R-tuple of D is nonnegative. In addition, the interest of Theorem 4.1 goes beyond its implications to secret sharing. The characterization of the representable discrete polymatroids was until now a open problem. Therefore, Theorem 4.1 is a interesting new result about representability of matroids.

Lemma 4.2 *From Proposition 2.3, observe that for all* $i, j \in J_m$, $\Delta r(i) = h(J_m) - h(J_m - \{i\}) \geq 0$, $\Delta r(i \cap j) = h(J_m - \{i\}) + h(J_m - \{j\}) - h(J_m - \{i, j\}) - h(J_m) \geq 0$ *and* $r(i \cap j) = h(\{i\}) + h(\{j\}) - h(\{i, j\}) \geq 0$. *This implies that when we apply Theorem 4.1 to* m*-partite matroids, for* $m \leq 2$ *all elements of the* R*-tuple of D are bound to nonnegative integers, but for* $m \geq 3$ *one or more negative integers may be present.*

Lemma 4.2 is very useful for the following examples.

5 An Example

In this section, we use an unipartite and a bipartite group communications as two examples to explain our result in Theorem 4.1.

First, by using Theorem 4.1 and Lemma 4.2, we show a new and simpler proof that all unipartite and bipartite matroids are representable, and hence, all access structures related to unipartite and bipartite representable matroids are ideal ones.

Example 5.1 Consider a discrete polymatroid D with ground set J_m and rank function $h : \mathcal{P}(J_m) \to \mathbb{Z}$.

For $m = 1$, $J_1 = \{1\}$ and $R = \{r(1)\}$. Observe that $r(1) = h(J_1) \geq 0$. Hence, the R-tuple of D is nonnegative and, then D is representable over some finite field.

For $m = 2$, $J_2 = \{1, 2\}$ and $R = \{\Delta r(1), \Delta r(2), r(1 \cap 2)\}$. Observe that $\Delta r(1) = h(J_2) - h(\{2\}) \geq 0$, $\Delta r(2) = h(J_2) - h(\{1\}) \geq 0$ and $r(1 \cap 2) = h(\{1\}) + h(\{2\}) - h(J_2) \geq 0$ (from Proposition 2.3). Hence, the R-tuple of D is nonnegative and, then D is representable over some finite field.

Similarly, from Lemma 4.2, we obtain that for $m \leq 2$ all elements of the R-tuple of D are bounded to be nonnegative integers, and hence, D is representable over some finite field.

As a consequence, we show a new and simpler proof that all unipartite and bipartite matroids are representable. It implies that access structures induced by unipartite and bipartite matroids are ideal, which has been done in [22], and also in [23,24].

Therefore, based on the method in Theorem 4.1, we can construct ideal unipartite and bipartite secret sharing schemes. Obviously, these unipartite and bipartite schemes are linear secret sharing schemes. Due to the fact that linear secret sharing schemes (LSSS) has an advantage over TSSS in terms of computational complexity while maintaining equal security (i.e., instead of computing a t-degree interpolating polynomial in TSSS, LSSS only needs to compute an inner product of two vectors). Thus, we can use idea unipartite and bipartite secret sharing schemes to design efficient and secure multipartite group solutions.

6 Conclusion

In this paper, we are motivated by exploring the possibility to develop ideal multipartite secret sharing schemes and use these schemes to design multipartite group keys establishment protocols. By introducing the new concept on the R-tuple of a discrete polymatroid, we obtain a new sufficient condition for a matroid to be representable, which implies a sufficient condition for an access structure to be ideal. Furthermore, we use an unipartite and a bipartite group communications as two examples to explain this sufficient condition. Our results are important for supporting efficient and secure multipartite-group-oriented applications.

References

1. Rafaeli, S., & Hutchison, D. (2003). A survey of key management for secure group communication. *ACM Computing Surveys*, *35*(3), 309–329.
2. Rodeh, O., Birman, K., & Dolev, D. (2001). The architecture and performance of security protocols in the ensemble group communication system. *ACM Transactions on Information and System Security*, *4*(3), 289–319.
3. Wong, C. K., Gouda, M. G., & Lam, S. S. (1998). Secure group communications using key graphs. *ACM SIGCOMM Computer Communication Review*, *28*, 68–79.
4. Sun, Y., & Liu, K. J. R. (2007). Hierarchical group access control for secure multicast communications. *Networking, IEEE/ACM Transactions*, *15*(6), 1514–1526.
5. McGrew, S. (2003). Key establishment in large dynamic groups using one-way function trees. *Software Engineering, IEEE Transactions*, *29*(5), 444–458.
6. Park, M. H., Park, Y. H., Jeong, H. Y., et al. (2013). Key management for multiple multicast groups in wireless networks. *IEEE Transactions on Mobile Computing*, *12*(9), 1712–1723.
7. Blakley, G. R. (1979). Safeguarding Cryptographic Keys. *Proceedings of American Federation of Information Processing Societies (AFIPS '79) National Computer Conference*, *48*, 313–317.
8. Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *24*(11), 612–613.
9. Harn, L. (2013). Group authentication. *IEEE Transaction on Computers*, *62*(9), 1893–1898.
10. Harn, L. (1995). Efficient sharing (broadcasting) of multiple secrets. *IEE Computers and Digital Techniques*, *142*(3), 237–240.
11. Harn, L. (1995). Comment multistage secret sharing based on one-way function. *Electronic Letters*, *31*(4), 262.
12. Hsu, Chingfang, Zeng, Bing, Cui, Guohua, & Chen, Liang. (2013). A new secure authenticated group key transfer protocol. *Wireless Personal Communications*. doi:10.1007/s11277-013-1298-2.
13. Laih, C., Lee, J., & Harn, L. (1989). A new threshold scheme and its application in designing the conference key distribution cryptosystem. *Information Processing Letters*, *32*, 95–99.
14. Berkovits, S. (1991). "How to broadcast a secret", Proceedings Eurocrypt '91 Workshop Advances in Cryptology, pp. 536–541.
15. Li, C.H., & Pieprzyk, J. (1999). "Conference Key Agreement from Secret Sharing", Proceedings of Fourth Australasian Conference Information Security and Privacy (ACISP '99), pp. 64–76.
16. Saze, G. (2003). Generation of key predistribution schemes using secret sharing schemes. *Discrete Applied Mathematics*, *128*, 239–249.
17. Harn, L., & Lin, C. (2010). Authenticated group key transfer protocol based on secret sharing. *Computers, IEEE Transactions*, *59*(6), 842–846.
18. IEEE Standard 802.16-2004. (2004). Part 16: Air interface for fixed broadband wireless access systems, IEEE.
19. Karnin, E. D., Greene, J. W., & Hellman, M. E. (1983). On secret sharing systems. *Information Theory, IEEE Transactions*, *29*(1), 35–41.
20. Beimel, A., Tassa, T., & Weinreb, E. (2008). Characterizing ideal weighted threshold secret sharing. *SIAM Journal on Discrete Mathematics*, *22*(1), 360–397.
21. Morillo, P., Padro, C., Saez, G., & Villar, J. L. (1999). Weighted threshold secret sharing schemes. *Information Processing Letters*, *70*, 211–216.
22. Padro, C., & Saez, G. (2000). Secret sharing schemes with bipartite access structure. *Information Theory, IEEE Transactions*, *46*, 2596–2604.

23. Ng, S.-L. (2003). A representation of a family of secret sharing matroids. *Designs, Codes and Cryptography*, *30*, 5–19.
24. Ng, S.-L., & Walker, M. (2001). On the composition of matroids and ideal secret sharing schemes. *Designs, Codes and Cryptography*, *24*, 49–67.
25. Herranz, J., & Saez, G. (2006). New results on multipartite access structures. *IEE Proceedings of Information Security*, *153*, 153–162.
26. Collins, M.J. A. (2002). Note on ideal tripartite access structures. Cryptology ePrint Archive, Report 2002/193, http://eprint.iacr.org/2002/193
27. Farràs, Oriol, Martí-Farré, Jaume, & Padró, Carles. (2012). Ideal multipartite secret sharing schemes. *Journal of Cryptology*, *25*(3), 434–463.
28. Farras, O., & Padro, C. (2012). Ideal hierarchical secret sharing schemes. *Information Theory, IEEE Transactions*, *58*(5), 3273–3286.
29. Farràs, O., Padró, C., Xing, C., & Yang, A. (2011). *Natural generalizations of threshold secret sharing* (pp. 610–627). ASIACRYPT.
30. Hsu, Chingfang, Tang, Xueming, Cheng, Qi, & Xiao, Haijun. (2010). Multipartite matroids and secret sharing. *Chinese Science Bulletin*, *55*(29), 3261–3266.
31. Brickell, E. F., & Davenport, D. M. (1991). On the classification of ideal secret sharing schemes. *Journal of Cryptology*, *4*(73), 123–134.
32. Herzog, J., & Hibi, T. (2002). Discrete polymatroids. *Journal of Algebraic Combinatorics*, *16*, 239–268.

Ching-Fang Hsu was born in Hubei, China, on Nov. 22, 1978. She received the M.Eng. and the Ph.D. degrees in information security from the Huazhong University of Science and Technology, Wuhan, China, in 2006 and 2010 respectively. From Sep. 2010 to Mar. 2013, she was a Research Fellow at the Huazhong University of Science and Technology. She is currently an Assistant Professor at Central China Normal University, Wuhan, China. Her research interests are in cryptography and network security, especially in secret sharing and its applications.

Shan Wu was born in Hubei, China, on Oct. 30, 1979. She received the M.Eng. and the Ph.D. degrees in information security from the Huazhong University of Science and Technology, Wuhan, China, in 2006 and 2010 respectively. She is currently an Assistant Professor at Wuhan Technology and Business University, Wuhan, China. She is currently investigating new ways of using secret sharing in various applications.

Lein Harn received the B.S. degree in electrical engineering from the National Taiwan University in 1977, the M.S. degree in electrical engineering from the State University of New York-Stony Brook in 1980, and the Ph.D. degree in electrical engineering from the University of Minnesota in 1984. In 1984, he joined the Department of Electrical and Computer Engineering, University of Missouri- Columbia as an assistant professor, and in 1986, he moved to Computer Science and Telecommunication Program (CSTP), University of Missouri, Kansas City (UMKC). While at UMKC, he went on development leave to work in Racal Data Group, Florida for a year. His research interests include cryptography, network security, and wireless communication security. He has published a number of papers on digital signature design and applications and wireless and network security. He has written two books on security. He is currently investigating new ways of using secret sharing in various applications.