EPiC Series in Computing

Volume 111, 2026, Pages 135–146

Proceedings of The 21st Asia Joint Conference on Information Security

Matroid Characterization and Ideal Secret Sharing for Complete t-Partite k-Uniform Hypergraph Access Structures

Chunming Tang[1], Zheng Chen[1]*, Haonan Fu[1], and Hongwei Zhu[1]

School of Mathematics and Information Science, Guangzhou, Guangdong, 510006, China
ctang@gzhu.edu.cn, zchen@e.gzhu.edu.cn,
haonanfu@e.gzhu.edu.cn, hongweizhu@gzhu.edu.cn

Abstract

Secret sharing schemes are an important class of cryptographic protocols, and linear codes are one of the main tools for constructing such schemes. This paper presents a matroid characterization and the construction of an ideal secret sharing scheme for complete t-partite k-uniform hypergraph access structures. First, we present a representable connected matroid and prove that the complete t-partite k-uniform hypergraph access structure is exactly the port of this matroid. Then, based on the theory of Brickell and Davenport on matroids and ideal access structures, and using linear codes as a tool, we give an ideal secret sharing scheme that realizes this access structure. This scheme unifies Shamir's threshold scheme and the complete t-partite graph scheme of Brickell et al. as special cases.

1 Introduction

Since their introduction by Shamir [13] and Blakley [2], secret sharing schemes have become a fundamental tool in cryptography. Ito et al. [7] proved that any monotone access structure can be realized by a secret sharing scheme, but general constructions suffer from low information rates. For graph-based access structures, where authorized sets correspond bijectively to edges, researchers have been able to reduce the information rate problem to the analysis of combinatorial properties of graphs. Brickell et al. [5] showed that complete multipartite graph access structures can be realized by ideal secret sharing schemes, assigning the same share to each clique using a threshold scheme. Subsequently, Brickell et al. [4] studied graph decompositions to obtain decompositions of the corresponding access structures and derived improved lower bounds on the information rate. Blundo et al. [3] developed the graph decomposition method of Brickell et al. [5, 4], and Di Crescenzo and Galdi [6] extended the idea to hypergraphs.

Linear codes serve as an important tool for constructing secret sharing schemes. McEliece and Sarwate [10] revealed the connection between Reed–Solomon codes and Shamir's threshold

*Zheng Chen is the corresponding author.

scheme. Massey [9] proposed a secret sharing scheme based on linear codes. In 2025, Tang et al. [14] gave a construction of optimal binary linear codes realizing arbitrary access structures, building upon Massey's scheme.

Brickell and Davenport [5] established that an ideal access structure must be the port of a unique connected matroid, and conversely, if an access structure is the port of a representable matroid over some field, then it is ideal. However, there exist matroid ports that are non-ideal (e.g., the port of the Vámos matroid [12]), so the general characterization of ideal access structures remains open. Nevertheless, several specific families have been fully characterized, including hierarchical threshold access structures [16], graph access structures [5], bipartite access structures [11], and access structures with three or four minimal authorized sets [8]. All these characterizations indicate that ideal access structures are realizable by linear schemes.

However, as a natural generalization of hypergraphs, the matroid characterization problem for complete t-partite k-uniform hypergraph access structures (see Definitions 2 and 3 in Section 2) has not yet been systematically studied. To this end, this paper makes a systematic study of this problem. Specifically, the main contributions of this paper are as follows:

- **Matroid characterization:** We give a connected representable matroid and prove that the complete t-partite k-uniform hypergraph access structure is the port of this matroid.
- **Realization of an ideal scheme:** Based on the above matroid and the work of Brickell and Davenport [5], using linear codes as a tool, we give an ideal secret sharing scheme for the complete t-partite k-uniform hypergraph access structure and prove its correctness and security.
- **Unification of existing work:** The $k = 2$ scheme of Brickell et al. [5] (the complete t-partite graph scheme) and Shamir's threshold scheme [13] are obtained as special cases of the above ideal secret sharing scheme.

The paper is organized as follows. Section 2 presents preliminary notions. Section 3 gives the matroid characterization. Section 4 describes the construction and its analysis. Section 5 discusses the proposed matroid and scheme. Section 6 concludes the paper and outlines future work.

2 Preliminaries

2.1 Access Structures and Secret Sharing Schemes

This subsection gives definitions related to complete t-partite k-uniform hypergraph access structures and secret sharing schemes.

Definition 1 (Access Structure)**.** Let $P = \{P_1, P_2, \ldots, P_n\}$ be a set of n participants, and let 2^P denote the set of all subsets of P. A non-empty subset $\Gamma \subseteq 2^P$ is called an **access structure** on P if it satisfies monotonicity:

$$\text{For any set } A \in \Gamma \text{ and any set } A' \in 2^P, \text{ if } A \subseteq A', \text{ then } A' \in \Gamma.$$

Define

$$\Gamma_{\min} = \{A \in \Gamma \mid \forall B \in 2^P,\ B \subsetneq A \Rightarrow B \notin \Gamma\}.$$

$\Gamma_{\min}$ is called the **minimal access structure** on P, and its elements are called **minimal authorized sets**. In secret sharing schemes, all authorized sets are generated by taking supersets

of the minimal authorized sets, so the minimal access structure uniquely determines the access structure. When no confusion arises, we also refer to $\Gamma_{\min}$ simply as the access structure.

Definition 2 (Complete t-Partite k-Uniform Hypergraph)**.** Let $V_1, \ldots, V_t$ be pairwise disjoint vertex sets with $|V_i| = n_i$. A hypergraph $G = (V, E)$ is called **complete t-partite k-uniform hypergraph** if

$$V = V_1 \cup \cdots \cup V_t,$$

and

$$E = \left\{ \{v_1, \ldots, v_k\} \subseteq V \mid v_j \in V_{i_j},\ \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, t\} \right\},$$

where $2 \leq k \leq t$. Each hyperedge contains exactly k vertices from k distinct vertex sets. When $k = 2$, this coincides with the classical complete t-partite graph.

Definition 3 (Complete t-Partite k-Uniform Hypergraph Access Structure)**.** Let $\Gamma_{\min}$ be a minimal access structure on participant set P. If $\Gamma_{\min}$ is represented as a hypergraph $G = (P, E)$ with $E = \Gamma_{\min}$, and G is complete t-partite k-uniform as in Definition 2 , then $\Gamma_{\min}$ is called a **complete t-partite k-uniform hypergraph access structure**.

Example 1. Let the participant set be

$$V = V_1 \cup V_2 \cup V_3 \cup V_4 \cup V_5 = \{P_{11}, P_{12}\} \cup \{P_{21}, P_{22}, P_{23}\} \cup \{P_{31}\} \cup \{P_{41}\} \cup \{P_{51}\}.$$

The complete 5-partite 3-uniform hypergraph access structure $\Gamma_{\min}$ consists of all 3-element subsets containing exactly one element from each of three distinct parts among $V_1, \ldots, V_5$. For instance, $\{P_{11}, P_{21}, P_{31}\} \in \Gamma_{\min}$, while $\{P_{11}, P_{12}, P_{21}\} \notin \Gamma_{\min}$. The entire set is determined by this rule.

Definition 4 (Adversary Structure)**.** Let P be the set of participants and $\Gamma \subseteq 2^P$ an access structure. A set B is called an **unauthorized set** if $B \in 2^P \setminus \Gamma$. An unauthorized set B is called a **maximal unauthorized set** if

$$\text{for any } B' \in 2^P \text{ with } B \subsetneq B',\ \text{we have } B' \in \Gamma.$$

Let $\mathcal{R}$ be the set of all maximal unauthorized sets on P. Then $\mathcal{R}$ is called the **adversary structure** corresponding to Γ.

For the definitions of information rate and perfect secret sharing schemes, we refer to Beimel's survey [1]. We recall that a scheme is called *ideal* if it is perfect and has information rate 1.

2.2 Linear Codes and Secret Sharing Schemes

Linear codes are an important tool for constructing secret sharing schemes. Their generator matrices naturally capture the linear relationship between the secret and the shares. This subsection gives definitions of linear codes and secret sharing schemes based on linear codes [9].

Definition 5 (Linear Code)**.** Let $\mathbb{F}_q$ be a finite field with q elements, and let $\mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$. If $C \subseteq \mathbb{F}_q^n$ is a k-dimensional subspace of $\mathbb{F}_q^n$, then C is called a q-ary $[n, k]$ **linear code**. If

$$a\mathbf{c} + \widetilde{a}\widetilde{\mathbf{c}} \in C, \quad \forall a, \widetilde{a} \in \mathbb{F}_q,\ \mathbf{c}, \widetilde{\mathbf{c}} \in C,$$

then each element $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ is called a codeword.

Since C is a k-dimensional subspace of $\mathbb{F}_q^n$, we can take k linearly independent codewords as rows to form a $k \times n$ matrix G, which is called a **generator matrix** of the linear code C.

The **dual code** of C is defined as

$$C^\perp = \{\mathbf{c}' \in \mathbb{F}_q^n \mid \forall \mathbf{c} \in C,\ \langle \mathbf{c}, \mathbf{c}' \rangle = 0\},$$

where $\langle \cdot, \cdot \rangle$ denotes the inner product. It is easy to see that if C is an $[n, k]$ linear code over $\mathbb{F}_q$, then $C^\perp$ is an $[n, n-k]$ linear code over $\mathbb{F}_q$. Similarly, $C^\perp$ has a generator matrix H, which is also a **parity-check matrix** of C.

Definition 6 (Secret Sharing Scheme Based on Linear Codes)**.** Let $G = (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_n)$ be a generator matrix of an $[n, k]$ linear code, where each $\mathbf{g}_i$ is a column vector in $\mathbb{F}_q^k$. Define a labeling map

$$\rho = \begin{pmatrix} 2 & 3 & \cdots & n+1 \\ P_1 & P_2 & \cdots & P_n \end{pmatrix},$$

where the first row gives the column indices of G and the second row gives the corresponding participants.

To share a secret $s \in \mathbb{F}_q$, the dealer chooses a random vector $\mathbf{u} \in \mathbb{F}_q^k$ such that $\mathbf{u}\mathbf{g}_0 = s$, computes $s_i = \mathbf{u}\mathbf{g}_i$ for each $i = 1, \ldots, n$, and sends s_i to P_i.

A set $S = \{P_{i_1}, \ldots, P_{i_m}\}$ can recover the secret iff there exist $h_{i_j} \in \mathbb{F}_q$, not all zero, such that

$$\mathbf{g}_0 = \sum_{j=1}^{m} h_{i_j} \mathbf{g}_{i_j},$$

in which case

$$s = \sum_{j=1}^{m} h_{i_j} s_{i_j}.$$

2.3 Ideal Secret Sharing Schemes and Matroids

In this subsection, we recall the formal definitions and lemmas from matroid theory that are needed for our characterization and construction. The two fundamental results of Brickell and Davenport [5] on ideal access structures are stated in Lemmas 1 and 2 below; for a detailed exposition, we refer to Beimel's survey [1].

Definition 7 (Matroid)**.** A matroid $\mathcal{M} = \langle V, r_\mathcal{M} \rangle$ consists of a finite set V and a function $r_\mathcal{M} : 2^V \to \mathbb{N}$ satisfying the following three axioms:

- **Non-negativity and boundness**: For any $X \subseteq V$, $0 \le r_\mathcal{M}(X) \le |X|$.
- **Monotonicity**: For any $X \subseteq Y \subseteq V$, $r_\mathcal{M}(X) \le r_\mathcal{M}(Y)$.
- **Sub-modularity**: $r_\mathcal{M}(X \cup Y) + r_\mathcal{M}(X \cap Y) \le r_\mathcal{M}(X) + r_\mathcal{M}(Y)$.

If $r_\mathcal{M}(X) = |X|$, then $X \subseteq V$ is called an **independent set**. If $r_\mathcal{M}(X) < |X|$, then $X \subseteq V$ is called a **dependent set**. If $A \subseteq V$ is a minimal dependent set (i.e., for every $a \in A$, $r_\mathcal{M}(A) = |A| - 1$ and $r_\mathcal{M}(A \setminus \{a\}) = |A| - 1$), then A is called a **circuit**. Moreover, if for every pair of distinct elements $x \in V$ and $y \in V$ there exists a circuit containing both x and y, then $\mathcal{M}$ is a **connected matroid**.

Definition 8 (Port of a Matroid)**.** Let $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ be a connected matroid, let $\mathcal{C}$ be the set of all circuits of $\mathcal{M}$, and let $P_0 \in V$. The **port** of $\mathcal{M}$ at point P_0 is the access structure $\Gamma_{\min}$ on the participant set $P = V \setminus \{P_0\}$ whose minimal authorized sets are

$$\{A \subseteq V \setminus \{P_0\} \mid A \cup \{P_0\} \in \mathcal{C}\}.$$

Definition 9 (Linearly Representable Matroid)**.** A matroid $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ is **linearly representable** over a field $\mathbb{F}$ if there exists a rank-preserving map from V to a set of vectors in some vector space over $\mathbb{F}$. That is, there exists an integer k and a map $\phi : V \to \mathbb{F}^k$ such that for every $A \subset V$, $r_{\mathcal{M}}(A) = \text{rank}(\phi(A))$, where rank denotes the linear algebra rank.

Lemma 1. ([5, Theorem 1]) Let $\Gamma_{\min}$ be a non-redundant access structure (every participant appears in at least one minimal authorized set) defined on a participant set P. If $\Gamma_{\min}$ is ideal, then there exists a connected matroid $\mathcal{M}$ defined on the finite set $P \cup \{P_0\}$ such that the port of $\mathcal{M}$ at P_0 is $\Gamma_{\min}$.

Lemma 2. ([5, Theorem 2]) If there exists a connected matroid $\mathcal{M}$ that is linearly representable over some field, then the non-redundant access structure derived from $\mathcal{M}$ can be realized by an ideal secret sharing scheme.

3 Matroid Characterization of Complete t-Partite k-Uniform Hypergraph Access Structures

In this section, for the complete t-partite k-uniform hypergraph access structure $\Gamma_{\min}$, we define a finite set $V = V_0 \cup P$, where $V_0 = \{P_0\}$ and $P = V_1 \cup \ldots \cup V_t$. Define a rank function $r_{\mathcal{M}}(X) = \min\{k, N(X)\}$, where $N(X) = |\{i \in \{0, 1, \ldots, t\} \mid V_i \cap X \neq \varnothing\}|$ denotes the number of distinct vertex sets covered by the set $X \subseteq V$. We prove that $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ is a connected matroid. We then show that $\mathcal{M}$ is linearly representable over a finite field $\mathbb{F}_q$ (with $q > t$) and that $\Gamma_{\min}$ is exactly the port of $\mathcal{M}$ at P_0.

We first verify that $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ defined in this way is indeed a matroid.

Lemma 3. $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ is a matroid.

Proof. We need to verify the three matroid axioms (see Definition 7).

Non-negativity and boundness: For any $X \subseteq V$, $0 \leq r_{\mathcal{M}}(X) \leq N(X) \leq |X|$.

Monotonicity: For any $X \subseteq Y \subseteq V$, since $N(X) \leq N(Y)$, we have $r_{\mathcal{M}}(X) \leq r_{\mathcal{M}}(Y)$.

Sub-modularity: By the inclusion–exclusion principle: $N(X \cup Y) + N(X \cap Y) = N(X) + N(Y)$. We discuss three cases based on the values of $N(X)$ and $N(Y)$ relative to k.

- **Case 1:** $N(X) \geq k$ and $N(Y) \geq k$. Then $r_{\mathcal{M}}(X \cup Y) = r_{\mathcal{M}}(X) = r_{\mathcal{M}}(Y) = k$ and $r_{\mathcal{M}}(X \cap Y) \leq k$.
- **Case 2:** $N(X) \geq k$ and $N(Y) \leq k$. Then $r_{\mathcal{M}}(X \cup Y) = r_{\mathcal{M}}(X) = k$, $r_{\mathcal{M}}(Y) = N(Y)$ and $r_{\mathcal{M}}(X \cap Y) \leq N(Y)$.
- **Case 3:** $N(X) \leq k$ and $N(Y) \leq k$. Then $r_{\mathcal{M}}(X) = N(X)$, $r_{\mathcal{M}}(Y) = N(Y)$, $r_{\mathcal{M}}(X \cap Y) = N(X \cap Y)$ and $r_{\mathcal{M}}(X \cup Y) \leq N(X \cup Y)$.

In all cases, we obtain

$$r_{\mathcal{M}}(X \cup Y) + r_{\mathcal{M}}(X \cap Y) \leq r_{\mathcal{M}}(X) + r_{\mathcal{M}}(Y).$$

Hence $\mathcal{M}$ satisfies all matroid axioms. □

Next, we consider the connectivity of $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$.

Lemma 4. The matroid $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ is connected.

Proof. We need to show that for any two distinct elements in V, there exists a circuit containing both. Consider two cases, without loss of generality.

- If the two elements belong to the same $V_i \subseteq V$, denote them by P_{i1} and P_{i2}. Let $A = \{P_{i1}, P_{i2}\}$. Since $N(A) = 1$, we have $r_{\mathcal{M}}(A) = 1 < |A| = 2$. For any $P_{ij} \in A$, $r_{\mathcal{M}}(A \setminus \{P_{ij}\}) = 1 = |A| = 2$. Thus A is a circuit of $\mathcal{M}$.
- If the two elements belong to different vertex sets V_i and V_j, denote them by P_{i1} and P_{j1}. Let A be a minimal authorized set containing P_{i1} and P_{j1} (such an A exists: when $k = 2$, $A = \{P_{i1}, P_{j1}\}$; when $k > 2$, add one participant from each of the other $k - 2$ vertex sets to A). Then the participants in A come from k distinct vertex sets. We have $r_{\mathcal{M}}(A) = k$ and removing any participant P_{ij} from A gives $r_{\mathcal{M}}(A \setminus P_{ij}) = k - 1$. Therefore $A \cup \{P_0\}$ is a circuit of $\mathcal{M}$.

Thus $\mathcal{M}$ is a connected matroid. □

We now prove that the above matroid $\mathcal{M}$ is linearly representable (see Lemma 5) and that the complete t-partite k-uniform hypergraph access structure $\Gamma_{\min}$ is the port of $\mathcal{M}$ at P_0 (see Theorem 1). Then we give an ideal linear secret sharing scheme for $\Gamma_{\min}$ (see Section 4).

Lemma 5. The connected matroid $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ is linearly representable over a finite field $\mathbb{F}_q$ with $q > t$.

Proof. In the vector space $\mathbb{F}_q^k$, select $t + 1$ one-dimensional subspaces $L_0, L_1, \ldots, L_t$ such that any k distinct basis vectors $\mathbf{g}_i$ from these subspaces are linearly independent. For example, choose distinct elements $x_0, x_1, \ldots, x_t \in \mathbb{F}_q$ and define

$$L_i = \operatorname{span}\{\mathbf{g}_i\} = \operatorname{span}\{\begin{pmatrix} 1 & x_i & x_i^2 & \cdots & x_i^{k-1} \end{pmatrix}\}.$$

Define the map $\phi : V \longrightarrow \mathbb{F}_q^k$ as follows: if $P_{ij} \in V_i$, let $\phi(P_{ij}) = c_{P_{ij}} \mathbf{g}_i$, where $c_{P_{ij}} \in \mathbb{F}_q^*$. For any $A \subseteq V$, if $N(A) > k$, then $r_{\mathcal{M}}(A) = k$. Meanwhile, $\phi(A)$ consists of vectors $\phi(P_{ij}) = c_{P_{ij}} \mathbf{g}_i$ for $P_{ij} \in A \cap V_i$, $i \in \{0, 1, \ldots, t\}$. These vectors come from more than k distinct subspaces L_i, so $\operatorname{rank}(\phi(A)) = r_{\mathcal{M}}(A) = k$. If $N(A) \leq k$, then $r_{\mathcal{M}}(A) = N(A)$. Similarly, $\phi(A)$ consists of vectors from $N(A)$ distinct subspaces L_i, so $\operatorname{rank}(\phi(A)) = r_{\mathcal{M}}(A) = N(A)$.

Hence $r_{\mathcal{M}}(A) = \operatorname{rank}(\phi(A))$ for all $A \subseteq V$, so ϕ is a representation of $\mathcal{M}$. □

Theorem 1. The complete t-partite k-uniform hypergraph access structure $\Gamma_{\min}$ is the port of the representable connected matroid $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ at P_0.

Proof. By the definition of a port (see Definition 8), it suffices to show that $A \subseteq V \setminus \{P_0\}$ is a minimal authorized set of $\Gamma_{\min}$ if and only if $A \cup \{P_0\}$ is a circuit of $\mathcal{M}$.

Suppose $A \subseteq V \setminus \{P_0\}$ is a minimal authorized set of $\Gamma_{\min}$. Then $|A| = k$ and the participants in A come from k distinct vertex sets, so $N(A) = k$. Consider $A \cup \{P_0\}$. We have

$$r_{\mathcal{M}}(A \cup \{P_0\}) = \min\{k, N(A \cup \{P_0\})\} = \min\{k, k+1\} = k < |A \cup \{P_0\}| = k + 1,$$

hence $A \cup \{P_0\}$ is a dependent set. For any $P_i \in A \cup \{P_0\}$:

- If $P_i = P_0$, then
$$r_{\mathcal{M}}(A) = \min\{k, N(A)\} = k = |A \cup \{P_0\}| - 1.$$

- If $P_i \neq P_0$, i.e., $P_i \in A$, then

$$r_{\mathcal{M}}\big((A \cup \{P_0\}) \setminus \{P_i\}\big) = \min\{k, N(A \setminus \{P_i\}) + 1\} = k = |A \cup \{P_0\}| - 1.$$

Therefore $A \cup \{P_0\}$ is a circuit of $\mathcal{M}$.

Suppose $A \cup \{P_0\}$ is a circuit of $\mathcal{M}$. Then

$$r_{\mathcal{M}}(A \cup \{P_0\}) = |A| \quad \text{and} \quad r_{\mathcal{M}}(A) = |A|.$$

That is,

$$\min\{k, N(A) + 1\} = |A| \quad \text{and} \quad \min\{k, N(A)\} = |A|.$$

We consider three cases:

- If $k \leq N(A)$, then from the above we get $|A| = k$. Since $N(A) \leq |A| = k$, we have $N(A) = k$. Thus A is a minimal authorized set of $\Gamma_{\min}$.
- If $k = N(A) + 1$, then the first equation gives $|A| = k = N(A) + 1$, while the second gives $|A| = N(A)$, a contradiction.
- If $N(A) + 1 < k$, then the first equation gives $|A| = N(A) + 1$ and the second gives $|A| = N(A)$, again a contradiction.

Hence only the first case holds, and A is a minimal authorized set of $\Gamma_{\min}$. □

4 Scheme Design for Complete t-Partite k-Uniform Hypergraph Access Structures

By Lemma 2 and Section 3, the complete t-partite k-uniform hypergraph access structure $\Gamma_{\min}$ is the port at P_0 of the representable connected matroid $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ over the finite field $\mathbb{F}_q$ ($q > t$). Thus there exists an ideal secret sharing scheme over that field realizing $\Gamma_{\min}$. We now explicitly give such a scheme using linear codes (see Section 2.2), where the column vectors of the generator matrix come from the linear representation of $\mathcal{M}$.

In this section, we first give the adversary structure $\mathcal{R}$ corresponding to the complete t-partite k-uniform hypergraph access structure, then present the ideal secret sharing scheme, analyze its correctness and security, and finally give an example.

4.1 Adversary Structure of the Complete t-Partite k-Uniform Hypergraph Access Structures

For a general access structure, computing the corresponding adversary structure $\mathcal{R}$ is difficult, and vice versa [15]. However, for the complete t-partite k-uniform hypergraph access structure, we have the following result.

Theorem 2. The adversary structure $\mathcal{R}$ corresponding to the complete t-partite k-uniform hypergraph access structure is

$$\mathcal{R} = \Big\{ \bigcup_{i \in J} V_i \;\Big|\; J \subseteq \{1, 2, \ldots, t\},\ |J| = k - 1 \Big\}.$$

Proof. For any $\bigcup_{i\in J} V_i$ with $|J| = k-1$, it does not contain any minimal authorized set, hence it is unauthorized. If we add any participant P' not in this vertex set, then the set $\bigcup_{i\in J} V_i \cup \{P'\}$ contains participants from k distinct vertex sets, so it becomes authorized. Thus each $\bigcup_{i\in J} V_i$ is a maximal unauthorized set.

Suppose there exists another maximal unauthorized set $B' \notin \mathcal{R}$. Then B' must be completely contained in some $\bigcup_{i\in J} V_i$ with $|J| = k-1$; otherwise, if B' covers at least k distinct vertex sets, then B' itself would contain a minimal authorized set, contradicting the maximality of B'. If B' is a proper subset of $\bigcup_{i\in J} V_i$, then there exists a participant $P^* \in \bigcup_{i\in J} V_i \setminus B'$. Consider $B' \cup \{P^*\}$. It is still completely contained in $\bigcup_{i\in J} V_i$ and thus remains unauthorized, contradicting the fact that B' is a maximal unauthorized set. Therefore B' must equal $\bigcup_{i\in J} V_i$, i.e., no other maximal unauthorized set exists. □

Example 2 (Example 1 continued)**.** The adversary structure corresponding to $\Gamma_{\min}$ in Example 1 is:

$$\begin{aligned}\mathcal{R} = &\{V_1 \cup V_2,\ V_1 \cup V_3,\ V_1 \cup V_4,\ V_1 \cup V_5\}\\ &\cup \{V_2 \cup V_3,\ V_2 \cup V_4,\ V_2 \cup V_5\}\\ &\cup \{V_3 \cup V_4,\ V_3 \cup V_5\}\\ &\cup \{V_4 \cup V_5\}.\end{aligned}$$

4.2 Secret Sharing Scheme for Complete t-Partite k-Uniform Hypergraph Access Structures

The scheme in this subsection is based on Lemma 2. Specifically, we take the map ϕ given in Lemma 5 as column vectors of the generator matrix (where P_0 corresponds to the first column $\mathbf{g}_0$, and each participant $P_{ij} \in V_i$ corresponds to $\phi(P_{ij})$), and follow Definition 6 for secret distribution and reconstruction.

Parameter selection.

Choose a finite field $\mathbb{F}_q$ with $q > t$. Let the participant set P be partitioned into t disjoint vertex sets $V_1, \ldots, V_t$, where $V_i = \{P_{i1}, P_{i2}, \ldots, P_{in_i}\}$, $|V_i| = n_i$ and total number of participants $n = \sum_{i=1}^{t} n_i$.

Secret distribution.

1. Choose a random vector: uniformly and randomly select $\mathbf{u} = \begin{pmatrix} u_1 & u_2 & \cdots & u_k \end{pmatrix} \in \mathbb{F}_q^k$ such that $\mathbf{u}\mathbf{g}_0 = s$.

2. For each participant $P_{ij} \in V_i$, compute $\phi(P_{ij}) = c_{P_{ij}}\mathbf{g}_i$, where $c_{P_{ij}} \in \mathbb{F}_q^*$. Denote $\mathbf{g}_{ij} = \phi(P_{ij})$. Then let $\mathbf{g}_{ij}$ be a column of the generator matrix G, and label that column by P_{ij}. Thus the public generator matrix G of size $k \times (n+1)$ is:

$$G = \begin{pmatrix} \mathbf{g}_0 & \mathbf{g}_{11} & \cdots & \mathbf{g}_{1n_1} & \cdots & \mathbf{g}_{t1} & \cdots & \mathbf{g}_{tn_t} \end{pmatrix},$$

   with labeling map

$$\rho = \begin{pmatrix} 2 & 3 & \cdots & n+1 \\ P_{11} & P_{12} & \cdots & P_{tn_t} \end{pmatrix},$$

   where the first row gives the column indices of G and the second row the corresponding participants.

3. For each participant $P_{ij} \in V_i$, the dealer computes $s_{ij} = \mathbf{u}\mathbf{g}_{ij}$ and sends the share s_{ij} to P_{ij}.

Secret reconstruction.
Let $A = \{P_{i_1j_1}, \ldots, P_{i_kj_k}\}$ be a minimal authorized set coming from k distinct vertex sets $V_{i_1}, \ldots, V_{i_k}$, with corresponding column vectors $\mathbf{g}_{i_1j_1}, \ldots, \mathbf{g}_{i_kj_k}$. Since these k column vectors belong to distinct one-dimensional subspaces, they form a basis of $\mathbb{F}_q^k$. It is easy to see that there exist coefficients $c_{i_1}, \ldots, c_{i_k} \in \mathbb{F}_q^*$, all non-zero, such that

$$\mathbf{g}_0 = c_{i_1}\mathbf{g}_{i_1j_1} + \cdots + c_{i_k}\mathbf{g}_{i_kj_k}.$$

During reconstruction, the participant set $\{P_{i_1j_1}, \ldots, P_{i_kj_k}\}$ can recover the secret using the reconstruction method of the linear code based secret sharing scheme.

Theorem 3 (Perfect Correctness)**.** In the scheme of Section 4.2, any set of participants that contains participants from at least k distinct vertex sets can correctly reconstruct the secret.

Proof. Let $A = \{P_{i_1j_1}, \ldots, P_{i_kj_k}\}$ contain participants from k distinct vertex sets $V_{i_1}, \ldots, V_{i_k}$ (not necessarily exactly k participants; if more than k participants are present, a subset of size k from distinct vertex sets suffices). The corresponding column vectors $\mathbf{g}_{i_1j_1}, \ldots, \mathbf{g}_{i_kj_k}$ form a basis of $\mathbb{F}_q^k$, so there exist non-zero coefficients $c_{i_1}, \ldots, c_{i_k} \in \mathbb{F}_q^*$ such that

$$\mathbf{g}_0 = c_{i_1}\mathbf{g}_{i_1j_1} + \cdots + c_{i_k}\mathbf{g}_{i_kj_k}.$$

Then

$$s = \mathbf{u}\mathbf{g}_0 = \sum_{l=1}^{k} c_{i_l}(\mathbf{u}\mathbf{g}_{i_lj_l}).$$

Thus A can reconstruct the secret. □

Theorem 4 (Perfect Security)**.** In the scheme of Section 4.2, for any participant set B whose members come from at most $k-1$ distinct vertex sets, no information about the secret s can be obtained.

Proof. Suppose the participants in B come from vertex sets $V_{i_1}, V_{i_2}, \ldots, V_{i_d}$ with $d \le k-1$. By the scheme of Section 4.2, participants within the same vertex set have column vectors belonging to the same one-dimensional subspace, and basis vectors from distinct vertex sets are linearly independent. Denote the basis vectors corresponding to these vertex sets as $\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_d}$. Then for any participant $P_{i_lj_l} \in B$, the share is $s_{i_lj_l} = \mathbf{u}\mathbf{g}_{i_lj_l}$ with $\mathbf{g}_{i_lj_l} \in \mathrm{span}\{\mathbf{g}_{i_l}\}$.

Consequently, the subspace spanned by all column vectors corresponding to B is contained in $\mathrm{span}\{\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_d}\}$. Since any k basis vectors from distinct subspaces are linearly independent and $d+1 \le k$, the vectors $\mathbf{g}_0, \mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_d}$ are linearly independent. Hence

$$\mathbf{g}_0 \notin \mathrm{span}\{\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_d}\} \supseteq \mathrm{span}\{\mathbf{g}_{i_lj_l} \mid P_{i_lj_l} \in B\}.$$

According to Massey's theory [9] on secret sharing based on linear codes (see Definition 6), a set of participants can reconstruct the secret if and only if $\mathbf{g}_0$ belongs to the subspace spanned by the column vectors corresponding to that set. If $\mathbf{g}_0$ is not in that subspace, then the secret cannot be reconstructed, and the distribution of shares is independent of the secret value. Therefore B obtains no information about the secret. □

Moreover, since both the secret and all shares are taken from the same finite field $\mathbb{F}_q$, the information rate is 1, so the scheme is ideal.

4.3 A Concrete Example

Example 3 (Example 1 continued)**.** Choose the finite field $\mathbb{F}_{11}$. In $\mathbb{F}_{11}^3$, select the following subspaces:

$$L_0 = \text{span}\left\{\begin{pmatrix}1\\0\\0\end{pmatrix}\right\},\ L_1 = \text{span}\left\{\begin{pmatrix}1\\1\\1\end{pmatrix}\right\},\ L_2 = \text{span}\left\{\begin{pmatrix}1\\2\\4\end{pmatrix}\right\},$$

$$L_3 = \text{span}\left\{\begin{pmatrix}1\\3\\9\end{pmatrix}\right\},\ L_4 = \text{span}\left\{\begin{pmatrix}1\\4\\5\end{pmatrix}\right\},\ L_5 = \text{span}\left\{\begin{pmatrix}1\\5\\3\end{pmatrix}\right\}.$$

Based on these subspaces, publish the generator matrix

$$G = \begin{pmatrix}1 & 2 & 1 & 2 & 3 & 1 & 1 & 1 & 1\\ 0 & 2 & 1 & 4 & 6 & 2 & 3 & 4 & 5\\ 0 & 2 & 1 & 8 & 1 & 4 & 9 & 5 & 3\end{pmatrix},$$

with labeling map

$$\rho = \begin{pmatrix}2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ P_{11} & P_{12} & P_{21} & P_{22} & P_{23} & P_{31} & P_{41} & P_{51}\end{pmatrix},$$

where $V_1 = \{P_{11}, P_{12}\}$, $V_2 = \{P_{21}, P_{22}, P_{23}\}$, $V_3 = \{P_{31}\}$, $V_4 = \{P_{41}\}$, $V_5 = \{P_{51}\}$.

Next, the dealer follows the scheme described in Section 4.2 to compute shares for each participant P_{ij} and send them securely. Any set of participants containing participants from at least three distinct vertex sets can reconstruct the secret using the reconstruction method of Section 4.2; any set containing participants from at most two distinct vertex sets obtains no information about the secret.

5 Discussion

5.1 Relationship with Existing Schemes

This section systematically compares the secret sharing scheme for complete t-partite k-uniform hypergraph access structures (see Section 4) with Shamir's threshold scheme [13] and the scheme of Brickell et al. [5].

Brickell et al. [5] gave an ideal secret sharing scheme for complete t-partite 2-uniform hypergraph access structures (i.e., complete t-partite graph access structures). Specifically, they pointed out that for a complete t-partite graph access structure, one can treat each vertex set as a "participant" and assign shares to such "participants" using a threshold scheme, while participants within the same vertex set receive the same share. We refer to the Brickell et al. scheme as the "copy threshold scheme method".

This paper extends the above structure from $k = 2$ to general k (with $2 \le k \le t$), i.e., complete t-partite k-uniform hypergraph access structures. In particular, when $k = 2$ and participants within the same vertex set V_i are assigned the same column vector in the scheme of Section 4.2, our scheme becomes exactly the "copy threshold scheme method" of Brickell et al. Therefore, we regard the scheme of Brickell et al. as a special case of our scheme.

Furthermore, for (k, t) threshold access structures, Shamir [13] gave an ideal scheme based on polynomial interpolation. From the perspective of our work, when each vertex set contains exactly one participant (i.e., $n_1 = \ldots = n_t = 1$), the complete t-partite k-uniform hypergraph access structure is exactly the (k, t) threshold access structure.

5.2 Further Discussion

It should be emphasized that the main contribution of this paper is not to propose a new scheme that is information-theoretically superior to existing ones, but rather to prove that the complete t-partite k-uniform hypergraph access structure is the port of the representable connected matroid $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ at P_0, and thereby to unify the complete t-partite k-uniform hypergraph access structure, the complete multipartite graph access structure, and the threshold access structure as special cases of the same matroid under different parameter settings. Based on the linear representation of the above matroid, we use linear codes and the Brickell–Davenport theory [5] to bridge the gap from matroid characterization to concrete scheme construction. The resulting scheme shows that by choosing different parameters, it realizes the complete t-partite k-uniform hypergraph access structure, the complete multipartite graph access structure, and the threshold access structure.

In terms of efficiency, the distribution complexity of our scheme is $O(k \cdot n)$ multiplications over the finite field, where $n = \sum_{i=1}^{t} n_i$ is the total number of participants. For reconstruction, since an authorized set contains exactly k participants, the reconstruction complexity is $O(k^2)$. The information rate is 1. Since the generator matrix is public, shares within the same vertex part can be mutually derived, which exactly matches the "intra-group trust, inter-group isolation" scenario, making the scheme suitable for applications such as cross-departmental approval and multi-institutional joint control that require multi-party collaboration. As a linear secret sharing scheme, our scheme supports additive homomorphism (linear combinations of secrets correspond to linear combinations of shares), but does not support multiplicative homomorphism.

6 Conclusion

In this paper, for the complete t-partite k-uniform hypergraph access structure $\Gamma_{\min}$, we defined a matroid $\mathcal{M} = \langle V, r_{\mathcal{M}} \rangle$ on the finite set $V = V_0 \cup V_1 \cup \ldots \cup V_t$ with $r_{\mathcal{M}}(X) = \min\{k, N(X)\}$. We proved that $\mathcal{M}$ is a connected matroid and is linearly representable over a finite field $\mathbb{F}_q$ (with $q > t$), and then proved that $\Gamma_{\min}$ is exactly the port of $\mathcal{M}$ at P_0. Based on these results and Lemma 2, we gave an ideal secret sharing scheme for $\Gamma_{\min}$ using linear codes, proved its correctness and security, and finally discussed the relationship between our scheme and existing schemes.

However, hypergraph access structures are often complex. For complex hypergraphs, how to construct secret sharing schemes with good information rate remains an open problem [6]. Inspired by the work of Blundo et al. [3] and Di Crescenzo et al. [6], we plan to consider whether any complex hypergraph can be decomposed into multiple simple sub-hypergraphs, especially complete t-partite k-uniform hypergraphs. If so, it would be promising to combine the schemes for these simple structures to construct secret sharing schemes with better information rate and further analyze the bounds on the information rate.

Acknowledgments

This research was supported by the National Natural Science Foundation of China under Grants 12571572, 12171114, and 12501728, and by the China Postdoctoral Science Foundation under Grant 2025M783088.

References

[1] Amos Beimel. Secret-sharing schemes for general access structures: An introduction. Cryptology ePrint Archive, 2025. Available at https://eprint.iacr.org/.

[2] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the 1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318, 1979.

[3] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *Journal of Cryptology*, 8:39–64, 1995. Preliminary version appeared in Advances in Cryptology – EUROCRYPT '92, R. A. Rueppel, ed., Lecture Notes in Computer Science 658, pp. 1–24, 1993.

[4] E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *Journal of Cryptology*, 5(3):153–166, 1992. Preliminary version in *Advances in Cryptology — CRYPTO '90*, Lecture Notes in Computer Science, vol. 537, pp. 242–252, 1990/1991.

[5] Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, 4(2):123–134, 1991.

[6] G. Di Crescenzo and C. Galdi. Hypergraph decomposition and secret sharing. *Discrete Applied Mathematics*, 157(5):928–946, 2009.

[7] Mitsuru Ito, Akira Saito, and Takao Nishizeki. Multiple assignment scheme for sharing secret. *Journal of Cryptology*, 6(1):15–20, 1993. Preliminary version in *Proceedings of IEEE Global Communications Conference (GLOBECOM 1987)*, pp. 99–102, 1987.

[8] Jaume Martí-Farré and Carles Padró. Secret sharing schemes with three or four minimal qualified subsets. *Designs, Codes and Cryptography*, 34(1):17–34, 2005.

[9] J. L. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pages 276–279, 1993.

[10] R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed-Solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.

[11] Carles Padró and Germán Sáez. Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory*, 46:2596–2605, 2000.

[12] Paul D. Seymour. On secret-sharing matroids. *Journal of Combinatorial Theory, Series B*, 56:69–73, 1992.

[13] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[14] Chun-Ming Tang, Jing-Wen Miao, and Qiu-Xia Xu. Construction of optimal secret key sharing scheme for non-threshold access structure. *Journal of Cryptologic Research*, 12(6):1421–1429, 2025.

[15] Chunming Tang, Qiongxia Xu, and Gang Hu. Finding the maximal adversary structure from any given access structure. *Information Sciences*, 508:329–342, 2020.

[16] Tamir Tassa. Hierarchical threshold secret sharing. In *Theory of Cryptography Conference (TCC 2004)*, volume 2951 of *Lecture Notes in Computer Science*, pages 473–490. Springer, 2004.