

Dynamic Participant Updates to Access and Adversary Structures for Ideal Secret Sharing Schemes Based on Linear Codes

Xu Qiuxia¹ Tang Chunming² Yi Zongxiang¹

¹School of Mathematics and Systems Science, Guangdong Polytechnic Normal University, Guangzhou, China

²School of Mathematics and Information Science, Guangzhou University, Guangzhou, China

Abstract

The paper investigates secret sharing schemes based on linear codes, focusing primarily on the access structures and adversary structures arising from dynamic participant updates, as well as on whether such access structures can be realized by ideal linear secret sharing schemes. First, we characterize the maximal adversary structure corresponding to the access structure obtained by adding new participants to every authorized subsets of a given access structure. Second, we prove that the original access structure can be realized by a linear code $C(n+1)[n+1, k; q]$ if and only if the access structure obtained after adding ℓ new participants can be realized by a linear code $C(n+\ell+1)[n+\ell+1, k+\ell; q]$. In addition, we establish the correspondence between the codewords of these two linear codes. Furthermore, We prove that the original access structure can be realized by an ideal secret sharing scheme if and only if the expanded access structure can be realized by one as well. Finally, we demonstrate that every linear secret sharing scheme realizing a disjoint access structure is ideal. We also prove that access structures whose any two minimal authorized subsets share all but one participant can be realized by an ideal linear secret sharing scheme. In addition, we determine the adversary structure corresponding to this class of access structures. More generally, we obtain the maximal adversary structure when new participants are added to merely part of the minimal authorized subsets.

Keywords: access structure, adversary structure, linear code, ideal secret sharing scheme

1 Introduction

The rapid advancement of distributed systems, blockchains and cloud-based multi-party collaboration has rendered secure and efficient key management and data sharing in environments with dynamically changing participants a fundamental cryptographic challenge. Frequent participant arrivals and departures are common in distributed systems. Typical scenarios, including dynamic blockchain node deployment and elastic tenant access for cloud collaboration, impose strict demands on the flexibility and security of these systems. Meanwhile, advanced applications, such as cross-chain interaction and federated collaborative computing in the cloud, further aggravate the accompanying security threats. Any vulnerabilities in these schemes may lead to secret leakage, node collusion and other security incidents, resulting in massive economic losses and severe information security risks. Secret sharing is a classical cryptographic primitive that distributes a secret among multiple participants such that any authorized set can reconstruct the secret, while other unauthorized set gains no information about it. Due to this property, secret

⁰Email: xia_mi0622@126.com

⁰Email: ctang@gzhu.edu.cn

⁰Email: tpu01yzx@gmail.com

sharing has been widely used in group key agreement[1][2][3], intrusion-tolerant systems[4][5][6], distributed trusted computing[7][8], and related applications, making it a fundamental enabling technique for addressing security challenges in dynamic participant environments.

Secret sharing was independently introduced by Shamir and Blakley in 1979. They proposed (t, n) -threshold secret sharing schemes based on polynomial interpolation over finite fields[9] and hyperplane geometry [10], respectively. In threshold secret sharing schemes, all participants receive shares of equal size and have equal reconstruction privileges, which makes these schemes widely adopted. In many practical applications, however, participants may require differentiated privileges. General secret sharing schemes were subsequently introduced to realize more flexible access control among participants[11][12][13][14][15]. Let $\mathcal{P} = \{P_1, \dots, P_n\}$ be a finite set of participants, and S be a finite domain of secrets. A secret sharing scheme distributes a secret $s \in S$ among the participants by means of private shares, such that authorized subsets can recover the secret from their shares, whereas unauthorized subsets cannot reconstruct s . The family of subsets that are allowed to reconstruct the secret is called the access structure, usually denoted by $\Gamma \subseteq 2^{\mathcal{P}}$. A subset $A \subseteq \mathcal{P}$ is called authorized if $A \in \Gamma$; otherwise, it is called unauthorized. An access structure is assumed to be monotone increasing: if $A \in \Gamma$ and $A \subseteq B \subseteq \mathcal{P}$, then $B \in \Gamma$. It collects all authorized subsets $A \in \Gamma$ such that no proper subset of A is authorized, equivalently, Γ is the upward closure of $\Gamma_{\min}$, meaning the full access structure is uniquely determined by its minimal authorized subsets. Conversely, the collection $\mathcal{R} = 2^{\mathcal{P}} \setminus \Gamma$ consisting of all unauthorized subsets satisfies monotonic decrease: for any $B \in \mathcal{R}$ and $C \subseteq B$, we have $C \in \mathcal{R}$. The family $\mathcal{R}$ is called the adversary structure.

Access structures lie at the heart of secret sharing: they determine which subsets of participants are authorized to reconstruct the secret, and their design directly shapes the security, efficiency, and applicability of a secret sharing scheme. In many practical settings, however, the set of participants is not static. Instead, it may expand dynamically as system requirements evolve and new entities are admitted[16][17][18][19], such as newly added bookkeeping nodes in a blockchain network, newly onboarded partner tenants in a cloud collaboration platform, or newly authorized nodes in a distributed trusted computing system. In such dynamic environments, it is not sufficient merely to ensure that the enlarged access structure remains monotone. It is equally important to understand how the corresponding adversary structure evolves: in particular, how the maximal unauthorized subsets change as the system grows. This evolution directly determines the system's resilience against collusion and its overall security properties, and is therefore essential to maintaining security under dynamic expansion. Numerous scholars have therefore researched various secret sharing schemes tailored to adversary structures to enhance collusion resistance[20][21][22][23].

Determining whether a general access structure can be realized by an ideal linear secret sharing scheme, and constructing such a scheme when it exists, is a challenging problem. The information rate of ideal secret sharing schemes is optimal, as each share occupies the same storage space as the secret itself. Their optimal share size can reduce storage overhead and may facilitate efficient deployment in distributed environments. However, most existing studies have focused on the construction and characterization of ideal linear secret sharing schemes for static access structures. Existing work has not fully characterized the following issues for ideal linear secret sharing under participant expansion: whether access structures can be realized by ideal secret sharing schemes after the participant set changes; the relationships between codewords of linear codes implementing access structures before and after new participants are added; and the structural evolution of the adversary structure following the addition of new participants. These questions are closely related to the classical connection between linear codes and secret sharing schemes[24][25][26]. McEliece et al. observed that Shamir's threshold secret sharing scheme can be interpreted in terms of Reed-Solomon codes[27]. More precisely, the participant coordinates in the support of such a minimal dual codeword, excluding the secret coordinate, form a minimal authorized set[28]. This provides an algebraic way to study access

structures through linear codes. However, determining the minimal codewords of a general linear code is computationally difficult. Conversely, Tang et al. showed that, for a given access structure, finding a realizing linear code can be formulated as solving a system of equations, and they further proposed an algorithm for finding an optimal realizing code when no ideal linear realization exists[29]. All these pioneering works lay a solid theoretical foundation and further motivate our work focusing on ideal linear realizability and codeword correspondences under participant expansion.

The connection between linear codes and access structures provides a foundation for the study of ideal access structures. Even so, a complete characterization of ideal access structures remains an open problem, deeply intertwined with combinatorics and information theory. Accordingly, prior work has sought partial characterizations by studying specific classes of access structures, including hierarchical threshold access structures [30], graph access structures [13][29][31], bipartite access structures [32], and access structures with three or four minimal authorized subsets[33]. A common feature of these results is that the access structures characterized in these works can be realized by ideal linear secret sharing scheme. From a theoretical standpoint, however, the fact that an access structure is ideally realizable does not necessarily imply that it admits an ideal linear realization. linear schemes are generally more efficient and tractable from the perspective of explicit construction. Therefore, it is of both theoretical and practical significance to investigate conditions under which an arbitrary access structure can be realized by an ideal linear secret sharing scheme.

Motivated by these considerations, this paper studies ideal linear secret sharing schemes based on linear codes, with a focus on the evolution of access structures and their associated adversary structures when new participants are added. The main contributions of this paper are summarized as follows:

- We first derive an explicit characterization of the maximal unauthorized sets in the adversary structure induced by the access structure obtained when new participants are added to the authorized sets of the original access structure. The resulting adversary structure is the union of two families of subsets: the first family consists of all sets obtained by adding all new participants to each maximal unauthorized set of the original adversary structure; the second family comprises all sets that retain all original participants together with all new participants except one arbitrarily chosen new participant.
- We then prove that a given original access structure is realizable by the linear code $C(n+1)[n+1, k; q]$ if and only if the access structure obtained after introducing new participants are realizable by the linear code $C(n+l+1)[n+l+1, k+l; q]$. We also establish an explicit correspondence between the codewords of the two codes, thereby relating the coding structures before and after participant expansion.
- Furthermore, we show that an access structure defined on n participants can be realized by an ideal secret sharing realization using the linear code $C(n+1)[n+1, k; q]$ if and only if the corresponding new access structure after adding ℓ new participants can be realized by an ideal secret sharing realization using the code $C(n+l+1)[n+l+1, k+l; q]$. This establishes equivalent conditions for preserving ideality under participant addition.
- Finally, we show that linear secret sharing schemes realizing disjoint access structures are ideal, and that access structures whose minimal authorized subsets pairwise share all but one participant can be realized by ideal secret sharing schemes, and we derive the formal formulation of their corresponding adversary structures. More generally, we characterize the explicit expression of the maximal adversary structure when new participants are added to merely part of the minimal authorized subsets.

2 Preliminaries

This paper draws primarily on secret sharing theory, algebraic coding theory, and combinatorics. This subsection introduces the concepts and notation needed for the subsequent discussion, including access structures, adversary structures, authorized and unauthorized sets, information rate, and linear code based secret sharing schemes.

2.1 Access structure and Adversary structure

Definition 2.1. Let $\mathcal{P} = \{p_1, p_2, \dots, p_n\}$ be the set of participants, and $AS \subseteq 2^{\mathcal{P}}$ be a non-empty family of subsets of $2^{\mathcal{P}}$, where $2^{\mathcal{P}}$ denotes the power set of $\mathcal{P}$. We call AS an access structure on $\mathcal{P}$ if it satisfies the monotonicity condition:

If $A \in AS$, then for any $C \in 2^{\mathcal{P}}$ such that $A \subseteq C$, it holds that $C \in AS$.

If AS is an access structure on the participant set $\mathcal{P}$, every set in AS is referred to as an authorized subset on $\mathcal{P}$.

Definition 2.2. Any set in $2^{\mathcal{P}} \setminus AS$ is called an unauthorized subset on $\mathcal{P}$. The collection of all unauthorized subsets is referred to as the adversary structure on $\mathcal{P}$, denoted by NAS .

Obviously, $AS \cup NAS = 2^{\mathcal{P}}$ and $AS \cap NAS = \emptyset$.

Definition 2.3. $\Gamma_{\min}$ is called the minimal access structure of AS , if

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

and every set in $\Gamma_{\min}$ is referred to as a minimal authorized subset. Where no ambiguity exists, the minimal access structure $\Gamma_{\min}$ may be abbreviated as the access structure.

Remark 2.1. All access structures considered in this paper are assumed to be non-redundant, meaning that each participant appears in at least one minimal authorized subset.

Definition 2.4. $\mathcal{R}_{\max}$ is called the maximal adversary structure of NAS , if

$$\mathcal{R}_{\max} = \{A \in NAS \mid \forall B \in 2^{\mathcal{P}}, A \subsetneq B \Rightarrow B \in AS\},$$

and every set in $\mathcal{R}_{\max}$ is referred to as a maximal unauthorized subset.

Definition 2.5. An minimal access structure $\Gamma_{\min}$ is called a Disjoint Access Structure if $A \cap B = \emptyset$ holds for all distinct $A, B \in \Gamma_{\min}$.

Definition 2.6. Let Γ be an access structure on P . A participant $x \in P$ is called a veto participant with respect to Γ , if every subset $U \subseteq P$ that does not contain x is an unauthorized set, that is, $x \notin U \Rightarrow U \notin \Gamma$.

2.2 Secret Sharing Schemes

A secret sharing scheme consists of two phases: a sharing phase in which a dealer distributes shares to participants, and a reconstruction phase in which authorized subsets recover the secret.

Definition 2.7. A secret sharing scheme based on an access structure $\Gamma \subseteq 2^{\mathcal{P}}$ is a pair of protocols:

- (a) **Share protocol:** The dealer takes a secret $s \in \mathcal{S}$ and computes shares $(s_1, \dots, s_n)$ from the sets $\mathcal{S}_1, \dots, \mathcal{S}_n$, distributing share s_i to each participant $p_i \in \mathcal{P}$,
- (b) **Reconstruct protocol:** A set of participants $A \subseteq \mathcal{P}$ attempts to reconstruct the secret from their shares $\{s_i : i \in A\}$. If $A \in \Gamma$, the protocol successfully outputs the secret s .

A secret sharing scheme satisfies two fundamental requirements:

- **Correctness:** Any authorized subset in the access structure can reconstruct the secret s ,
- **Perfect security:** Any unauthorized subset in the adversary structure cannot reconstruct the secret s , and can obtain no information about s whatsoever

is called a perfect secret sharing scheme.

If a secret sharing scheme realizing Γ is perfectly secure and the share length of each participant equals the length of the secret, then the scheme is called an ideal secret sharing scheme. Furthermore, if the share distribution process is linear, the scheme is referred to as an ideal linear secret sharing scheme.

2.3 Linear Secret Sharing Schemes

McEliece et al. demonstrated that there is a one-to-one correspondence between threshold secret sharing schemes and Reed-Solomon codes [27]. Since then, fruitful results have been achieved in the research on linear codes and secret sharing schemes. This subsection mainly introduces the relationship between linear codes and general secret sharing schemes.

Definition 2.8. Let $\mathbb{F}_q^{n+1}$ be the $n+1$ dimensional vector space over the finite field $\mathbb{F}_q$. A linear code C is a k dimensional subspace of $\mathbb{F}_q^{n+1}$ with $k \leq n$, denoted as an $[n+1, k; q]$ code, where $n+1$ is the code length of the linear code C , k is the dimension of C , and q indicates that C is a q -ary code over the finite field $\mathbb{F}_q$. Each vector in C is called a codeword.

Definition 2.9. Let C be an $[n+1, k; q]$ linear code. Form a $k \times (n+1)$ matrix $\mathbb{G}$ whose rows consist of a basis of C :

$$\mathbb{G} = \begin{pmatrix} g_{1,0} & g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,0} & g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{k,0} & g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix} = (\mathbf{g}_0, \mathbf{g}_1, \dots, \mathbf{g}_n).$$

This matrix $\mathbb{G}$ is called the generator matrix of the linear code C .

From the above definition, every codeword in C is a linear combination of the row vectors of $\mathbb{G}$. Hence there are a total of q^k codewords in C .

Definition 2.10. Let C be an $[n+1, k; q]$ linear code. Its dual code is defined as

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_q^{n+1} \mid (\mathbf{x}, \mathbf{c}) = 0, \forall \mathbf{c} \in C\}.$$

Definition 2.11. Let C be an $[n+1, k; q]$ linear code over the finite field $\mathbb{F}_q$, and let $\mathbf{c} = (c_0, c_1, \dots, c_n) \in C$ be a codeword. The set $\text{supp}(\mathbf{c}) = \{i \in [0, n] \mid c_i \neq 0\}$ is called the support of the codeword $\mathbf{c}$. If the support of $\mathbf{c}$ contains the support of $\mathbf{v}$, we say that the codeword $\mathbf{c}$ covers the codeword $\mathbf{v}$.

Definition 2.12. A codeword $\mathbf{c} = (c_0, c_1, \dots, c_n) \in \mathbb{F}_q^{n+1}$ is called a minimal codeword with first coordinate 1 if

- $\mathbf{c}$ is nonzero and $c_0 = 1$;
- there exists no other codeword $\mathbf{c}'$ whose first component is also 1 that covers $\mathbf{c}$.

This section mainly introduces the method of constructing secret sharing schemes by linear codes.

In distribution phase, let $s \in \mathbb{F}_q$ be the secret shared among n participants $p_1, p_2, \dots, p_n$. To compute the shares of s , the dealer randomly selects a vector $\mathbf{u} = (u_0, u_1, \dots, u_{k-1}) \in \mathbb{F}_q^k$ such that $\mathbf{u}\mathbf{g}_0 = s$. The dealer computes the codeword $\mathbf{s} = (s_0, s_1, \dots, s_n) = \mathbf{u} \cdot \mathbb{G}$ in code C , and secretly sends the share s_i to participant p_i , for $i = 1, 2, \dots, n$.

In principle, any linear code can be used to construct a secret sharing scheme. Before discussing secret reconstruction, we first review a lemma in [34].

Lemma 2.1. *Let $\mathbb{G}$ be a generator matrix of the linear code C . In the secret sharing scheme based on linear code C , the set of keys $\{s_{i_1}, s_{i_2}, \dots, s_{i_m}\}$ can determine the master secret key s if and only if there exists a codeword in the dual code $C^\perp$ of the form*

$$(1, 0, \dots, 0, c_{i_1}, 0, \dots, 0, c_{i_m}, 0, \dots, 0), \quad (*)$$

where at least one j satisfies $c_{i_j} \neq 0$, $1 \leq i_1 \leq \dots \leq i_m \leq n$ and $1 \leq m \leq n$.

In the reconstruction phase, if such a codeword of the form given in Lemma 2.1 exists in $C^\perp$, then $\mathbf{g}_0$ is a linear combination of $\mathbf{g}_{i_1}, \mathbf{g}_{i_2}, \dots, \mathbf{g}_{i_m}$, i.e.,

$$\mathbf{g}_0 = \sum_{j=1}^m c_{i_j} \cdot \mathbf{g}_{i_j}.$$

Let $\{p_{i_1}, p_{i_2}, \dots, p_{i_m}\} \subseteq \mathcal{P}$ be a minimal authorized subset, such that these participants can jointly recover the secret s by computing

$$s = \mathbf{u} \cdot \mathbf{g}_0 = \mathbf{u} \cdot \sum_{j=1}^m c_{i_j} \cdot \mathbf{g}_{i_j} = \sum_{j=1}^m c_{i_j} \cdot (\mathbf{u} \cdot \mathbf{g}_{i_j}) = \sum_{j=1}^m c_{i_j} \cdot s_{i_j}.$$

The above lemma mainly illustrates the relationship between linear codes and general secret sharing schemes. In fact, each participant corresponds to a respective column of the generator matrix of the linear code, except for the first column. If a subset of participants can reconstruct the secret, then there exists a codeword in the dual code of this linear code whose first component is $\mathbf{1}$, with non-zero entries at the positions corresponding to this subset of participants. The access structure $\Gamma_{\min}$ realized by this scheme is linear, and the length of each participant's share is equal to the length of the secret. Hence, the scheme is ideal and the secret sharing scheme constructed above to realize $\Gamma_{\min}$ is an ideal linear secret sharing scheme.

3 Linear Codes for Given Access Structures and Shortened Codes

The matrix representation of access structures adopted hereinafter follows the construction proposed by Tang et al. in Reference[29]. Specifically, let $\mathcal{P} = \{1, 2, \dots, n\}$ denote the set of n participants, and $\Gamma = \{S_1, \dots, S_m\}$ be a minimal access structure defined on $\mathcal{P}$, where $S_i \subseteq \mathcal{P}$ for $1 \leq i \leq m$. Unless otherwise specified, Γ denotes the minimal access structure.

The access structure Γ can be expressed in matrix form as

$$\Gamma = \begin{pmatrix} h_{1,1} & h_{1,2} & \dots & h_{1,n} \\ h_{2,1} & h_{2,2} & \dots & h_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{m,1} & h_{m,2} & \dots & h_{m,n} \end{pmatrix}, \quad (1)$$

where $h_{ij} \neq 0$ if $j \in S_i$, and $h_{ij} = 0$, otherwise, for all $1 \leq i \leq m$ and $1 \leq j \leq n$. Each row of this matrix corresponds to an authorized subset, and each column is associated with an individual participant. If a participant is not contained within a given authorized subset of Γ , the entry at the intersection of the corresponding row and column is zero.

Meanwhile, we define the $m \times (n + 1)$ matrix $\mathbb{H}$ as follows:

$$\mathbb{H} = (\mathbf{1} \quad \Gamma) = \begin{pmatrix} 1 & h_{1,1} & h_{1,2} & \cdots & h_{1,n} \\ 1 & h_{2,1} & h_{2,2} & \cdots & h_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & h_{m,1} & h_{m,2} & \cdots & h_{m,n} \end{pmatrix} = \begin{pmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \\ \vdots \\ \mathbf{h}_m \end{pmatrix},$$

where $\mathbf{1}$ denotes an all-one column vector of length m .

Compared with the original matrix representation of Γ , the matrix $\mathbb{H}$ is augmented with an all-one column as the 0-th column, and The remaining columns are indexed from 1 to n . Every participant is contained in at least one authorized subset. Accordingly, $\mathbb{H}$ contains no all-zero column vectors, and participant i corresponds to the i -th column of the matrix, for $i = 1, \dots, n$.

Suppose the maximal adversary structure corresponding to the access structure Γ is $\mathcal{R} = \{R_1, \dots, R_t\}$.

Similarly, we define

$$\mathbb{G} = \begin{pmatrix} 1 & g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ 1 & g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & g_{t,1} & g_{t,2} & \cdots & g_{t,n} \end{pmatrix}$$

where $g_{ij} = 0$ if $j \in R_i$, and is a non-zero element otherwise. All access structures we consider are connected (i.e., every participant belongs to at least one authorized subset). By the properties of access structures and adversary structures, the matrix $\mathbb{G}$ defined above contains no all-zero columns (otherwise the corresponding participant would not be included in any authorized subset).

Theorem 3.1. *There exists a linear code realizing the given access structure $\Gamma_{\min} = \{S_1, \dots, S_m\}$ if and only if the following system of quadratic equations $\mathbb{G}\mathbb{H}^T = \mathbf{0}$ has a solution over $\mathbb{F}_q$ for the unknowns h_{ij} ($j \in S_i$) and g_{ij} ($j \notin R_i$), subject to the constraint that $h_{ij} \neq 0$ for all $j \in S_i$.*

Proof. See the references[29] for detaile. □

It follows from the above theorem that if a given access structure Γ can be realized by an ideal linear secret sharing scheme (a linear secret sharing scheme based on a linear code of length $n + 1$ is called ideal, where n denotes the number of participants), then the quadratic system of equations $\mathbb{G}\mathbb{H}^T = \mathbf{0}$ defined by the matrices $\mathbb{H}$ and $\mathbb{G}$ necessarily has a solution over the finite field $\mathbb{F}_q$. Conversely, if the quadratic system $\mathbb{G}\mathbb{H}^T = \mathbf{0}$ admits a solution, then there exists a linear code C of length $n + 1$ that realizes an ideal linear secret sharing scheme, whose underlying access structure is ideal, which implies that the original access structure Γ is an ideal access structure. Evidently, the linear code C is the subspace of $\mathbb{F}_q^{n+1}$ spanned by the row vectors of $\mathbb{G}$. Any two distinct columns of $\mathbb{G}$ are not scalar multiples over $\mathbb{F}_q$.

The above theorem provides a criterion for the linear secret sharing realization of an ideal access structure. Song[35] carried out research on minimal linear codes and constructed new minimal linear codes using shortened codes. Adopting a similar shortened code idea, this paper characterizes ideal linear secret sharing schemes via matrix equations corresponding to access structures and adversary structures, and explores the inherent relationship between codewords realizing the access structure after new participants are added. We first present the construction method of shortened codes.

Let C be an $[n+1, k; q]$ linear code, with information symbols placed at the first k positions, and its generator matrix is given by

$$\mathbb{G} = \begin{pmatrix} g_{10} & g_{11} & \cdots & g_{1,n-1} & g_{1,n} \\ g_{20} & g_{21} & \cdots & g_{2,n-1} & g_{2,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g_{k0} & g_{k1} & \cdots & g_{k,n-1} & g_{k,n} \end{pmatrix},$$

and no two columns of $\mathbb{G}$ are scalar multiples over $\mathbb{F}_q$.

For any linear code or vector space V over $\mathbb{F}_q$, we write $\dim V = \dim_{\mathbb{F}_q} V$ for its dimension as an $\mathbb{F}_q$ -vector space; equivalently, $\dim V$ is the number of vectors in any basis of V . If V is a linear code over $\mathbb{F}_q$, then

$$|V| = q^{\dim V}, \quad \dim V = \log_q |V|.$$

For a linear map T , $\text{rank } T$ denotes the dimension of its image: $\text{rank } T = \dim_{\mathbb{F}_q} \text{Im}(T)$.

Define $C(n+1) = \{c = (c_0, c_1, \dots, c_{n-1}, 0) \mid c \in C\}$. Thus $C(n+1)$ is the subcode of C consisting of all codewords whose $(n+1)$ -th coordinate is zero. It is still regarded as a linear code in $\mathbb{F}_q^{n+1}$. Furthermore, define

$$C(n+1)[n] = \{(c_0, c_1, \dots, c_{n-1}) \mid (c_0, c_1, \dots, c_{n-1}, 0) \in C(n+1)\}.$$

This is the usual shortening of C at the $(n+1)$ -th coordinate: one first restricts to codewords whose $(n+1)$ -th coordinate is zero and then deletes that coordinate.

Lemma 3.1. *Let C be an $[n+1, k; q]$ linear code such that any two columns of its generator matrix $\mathbb{G}$ are linearly non-proportional. Define $C(n+1) = \{\mathbf{c} = (c_0, c_1, \dots, c_{n-1}, 0) \mid \mathbf{c} \in C\}$, then*

1. $C(n+1)$ is a $[n+1, k-1; q]$ linear code;
2. $C(n+1)$ has a generator matrix of the form

$$\mathbb{G}(n+1) = \begin{pmatrix} g'_{20} & g'_{21} & \cdots & g'_{2,n-1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ g'_{k0} & g'_{k1} & \cdots & g'_{k,n-1} & 0 \end{pmatrix}$$

and none among the first n columns of $\mathbb{G}(n+1)$ is an all-zero column.

Proof. We first verify $C(n+1)$ is a subspace of C .

For any $x = (x_0, \dots, x_{n-1}, 0), y = (y_0, \dots, y_{n-1}, 0) \in C(n+1)$ and $a, b \in \mathbb{F}_q$, we have $ax + by = (ax_0 + by_0, \dots, ax_{n-1} + by_{n-1}, 0) \in C$, and its last coordinate is zero. Therefore, $ax + by \in C(n+1)$ and $C(n+1)$ is a linear code of length $n+1$.

We now show that $\dim C(n+1) = k-1$. Define the linear map

$$\varphi : C \longrightarrow \mathbb{F}_q, \quad \varphi(c_0, c_1, \dots, c_n) = c_n.$$

Clearly, $\ker \varphi = C(n+1)$. The $(n+1)$ -th column of $\mathbb{G}$ is nonzero, so there exists a row index s satisfying $g_{sn} \neq 0$. The row vector

$$(g_{s0}, g_{s1}, \dots, g_{s,n-1}, g_{sn})$$

is a codeword of C with a nonzero $(n+1)$ -th coordinate, which implies $\varphi \neq 0$. Since $\mathbb{F}_q$ is one-dimensional over itself, the image of a nonzero linear map from C to $\mathbb{F}_q$ equals the whole field $\mathbb{F}_q$, and so $\text{rank } \varphi = 1$.

From the rank-nullity theorem, we have $\dim C(n+1) = \dim C - \text{rank } \varphi = k-1$. Consequently, $C(n+1)$ is an $[n+1, k-1; q]$ linear code.

We now construct a generator matrix for $C(n+1)$. Since any two columns of $\mathbb{G}$ are linearly independent, $\mathbb{G}$ has no all-zero columns, so its $(n+1)$ -th column is nonzero. Without loss of generality, we assume $g_{1,n} \neq 0$.

For each integer r with $2 \leq r \leq k$, define $\mathbf{h}_r = (g_{r0}, \dots, g_{rn}) - \frac{g_{rn}}{g_{1n}}(g_{10}, \dots, g_{1n})$. We then have

$$\mathbf{h}_r = (g_{r0} - g_{1n}^{-1}g_{rn}g_{10}, \dots, g_{r,n-1} - g_{1n}^{-1}g_{rn}g_{1,n-1}, 0).$$

Let $g'_{ri} = g_{ri} - g_{1n}^{-1}g_{rn}g_{1i}$, $2 \leq r \leq k$, $0 \leq i \leq n-1$. Then $\mathbf{h}_2, \dots, \mathbf{h}_k \in C(n+1)$, and they are exactly the row vectors of the generator matrix

$$\mathbb{G}(n+1) = \begin{pmatrix} g'_{20} & g'_{21} & \cdots & g'_{2,n-1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ g'_{k0} & g'_{k1} & \cdots & g'_{k,n-1} & 0 \end{pmatrix}.$$

Now we claim that $\mathbf{h}_2, \dots, \mathbf{h}_k$ are linearly independent. Assume that $\sum_{r=2}^k a_r \mathbf{h}_r = 0$.

Then $\sum_{r=2}^k a_r \left(\mathbf{g}_r - \frac{g_{rn}}{g_{1n}} \mathbf{g}_1 \right) = 0$, that is, $\left(-\sum_{r=2}^k a_r \frac{g_{rn}}{g_{1n}} \right) \mathbf{g}_1 + \sum_{r=2}^k a_r \mathbf{g}_r = 0$, where $\mathbf{g}_1, \dots, \mathbf{g}_k$ denote the row vectors of $\mathbb{G}$. Since $\mathbb{G}$ is a k -dimensional generator matrix, its rows are linearly independent. Hence $a_2 = \dots = a_k = 0$. Thus $\mathbf{h}_2, \dots, \mathbf{h}_k$ are linearly independent. We have $k-1$ vectors inside the $(k-1)$ -dimensional space $C(n+1)$, so they form a basis of $C(n+1)$. This means $\mathbb{G}(n+1)$ generates the code $C(n+1)$.

Finally, we prove that none of the first n columns of $\mathbb{G}(n+1)$ is zero. We argue by contradiction: suppose there exists an index i satisfying $0 \leq i \leq n-1$ such that the i -th column of $\mathbb{G}(n+1)$ is all zero. Then for all $r = 2, \dots, k$,

$$g'_{ri} = g_{ri} - g_{1n}^{-1}g_{rn}g_{1i} = 0.$$

Hence $g_{ri} = g_{1n}^{-1}g_{1i}g_{rn}$ for all $r = 2, \dots, k$. The first row also satisfies $g_{1i} = g_{1n}^{-1}g_{1i}g_{1n}$. Accordingly, the i -th and n -th columns of the original generator matrix $\mathbb{G}$ satisfy $\mathbf{e}_i = \frac{g_{1i}}{g_{1n}} \mathbf{e}_n$.

Thus $\mathbf{e}_i$ and $\mathbf{e}_n$ are proportional, contradicting the hypothesis. Hence none of the first n columns of $\mathbb{G}(n+1)$ is zero. $\square$

Lemma 3.2. Let $C(n+1)[n] = \{ (c_0, c_1, \dots, c_{n-1}) \mid (c_0, c_1, \dots, c_{n-1}, 0) \in C(n+1) \}$, where $C(n+1)$ is defined as in Lemma 3. Then:

1. $C(n+1)[n]$ has the generator matrix

$$\mathbb{G}(n+1)[n] = \begin{pmatrix} g'_{20} & g'_{21} & \cdots & g'_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ g'_{k0} & g'_{k1} & \cdots & g'_{k,n-1} \end{pmatrix},$$

by removing the last zero column of $\mathbb{G}(n+1)$;

2. $C(n+1)[n]$ is an $[n, k-1; q]$ linear code.

Proof. Let the projection map $\pi : \mathbb{F}_q^{n+1} \rightarrow \mathbb{F}_q^n$ be defined by

$$\pi(c_0, c_1, \dots, c_{n-1}, c_n) = (c_0, c_1, \dots, c_{n-1}).$$

Then $C(n+1)[n] = \pi(C(n+1))$.

Since π is linear and $C(n+1)$ is a vector space, $C(n+1)[n]$ is a linear code over $\mathbb{F}_q^n$. Every codeword in $C(n+1)$ has a zero in the $(n+1)$ -th coordinate. Thus if $\pi(\mathbf{c}) = \mathbf{0}$ with $\mathbf{c} \in C(n+1)$, the first n entries of code $\mathbf{c}$ are zero, and its $(n+1)$ -th entry is also zero. Consequently, $\mathbf{c}$ must be the zero codeword. Thus the restriction of π to $C(n+1)$ is injective, and

$$\dim(C(n+1)[n]) = \dim C(n+1) = k-1.$$

However the length of $C(n+1)[n]$ is n , so it is an $[n, k-1; q]$ linear code.

It remains to identify its generator matrix. By Lemma 3, $C(n+1) = \{u\mathbb{G}(n+1) \mid u \in \mathbb{F}_q^{k-1}\}$.

For any $u \in \mathbb{F}_q^{k-1}$, the last column of $\mathbb{G}(n+1)$ is zero. Removing the zero coordinate, we have

$$\pi(u\mathbb{G}(n+1)) = u(\mathbb{G}(n+1)[n]).$$

Therefore $C(n+1)[n] = \{u(\mathbb{G}(n+1)[n]) \mid u \in \mathbb{F}_q^{k-1}\}$.

This implies $\mathbb{G}(n+1)[n]$ generates $C(n+1)[n]$. Since $\dim(C(n+1)[n]) = k-1$, its $k-1$ rows are linearly independent, and so $\mathbb{G}(n+1)[n]$ is a generator matrix of the shortened code. $\square$

The two lemmas above describe the shortening operation of a linear code with respect to a single specified coordinate: we first extract the subcode consisting of all codewords whose entry at this coordinate is zero, and then deletes this identically zero coordinate. In fact, when multiple coordinates that are uniformly zero for all codewords need to be eliminated simultaneously, this shortening procedure can be carried out iteratively. Subsequently, we adopt this procedure to characterize the relationship between the codewords corresponding to the original access structure and the access structure after adding new participants.

4 Ideal Linear Secret Sharing Schemes and Dynamic Participant Updates

We construct ideal secret sharing schemes based on the above linear codes and further investigate the variation of access structures when new participants are added.

4.1 Maximal Adversary Structure Characterisation for Dynamic Participant Updates

Theorem 4.1. *Let $\Gamma = \{S_1, S_2, \dots, S_m\}$ be an access structure on the participant set P , and $\mathcal{R}$ be the corresponding maximal adversary structure. Let $P' = \{p'_1, p'_2, \dots, p'_\ell\}$, $P \cap P' = \emptyset$, $\ell \geq 1$, and define the expanded access structure $\Gamma' = \{S_i \cup P' \mid S_i \in \Gamma\}$ on the participant set $P \cup P'$. Then the maximal adversary structure of Γ' is*

$$\mathcal{R}' = \{R_i \cup P' \mid R_i \in \mathcal{R}\} \cup \{P \cup (P' \setminus \{p'_j\}) \mid p'_j \in P'\}.$$

In particular, when $\ell = 1$, the second collection reduces to $\{P\}$.

Proof. By the above definition of Γ' , a subset $U \subseteq P \cup P'$ satisfies $U \in \Gamma'$ if and only if $P' \subseteq U$ and $U \cap P \in \Gamma$. Therefore, U is an unauthorized subset whenever $P' \not\subseteq U$ or $U \cap P \notin \Gamma$. Let $\mathcal{R}'$ denote the maximal adversary structure corresponding to Γ' , where $U \in \mathcal{R}'$ is a maximal unauthorized subset.

We now consider two cases.

Case 1: $P' \subseteq U$. Let $U = A \cup P'$, so that $A = U \cap P \subseteq P$.

Since $U \in \mathcal{R}'$, we have $A \notin \Gamma$. We claim that A is a maximal unauthorized subset of Γ .

Suppose there exists A' such that $A \subsetneq A' \subseteq P$ and $A' \notin \Gamma$. Then $A' \cup P' \notin \Gamma'$ and $U = A \cup P' \subsetneq A' \cup P'$. U is a maximal unauthorized subset, hence A is maximal unauthorized subset on P , so $A = R_i$ for some $R_i \in \mathcal{R}$. We obtain $U = R_i \cup P'$.

Case 2: $P' \not\subseteq U$. Therefore there exists at least one participant p'_j such that $p'_j \in P' \setminus U$. Let $U = A \cup B \subseteq P \cup P'$, then $A = U \cap P$, $B = U \cap P'$.

We first claim that $A \in \Gamma$. Suppose $A \notin \Gamma$.

Since $U \cap P = A \notin \Gamma$. By definition of Γ' , $U \cup \{p'_j\} \notin \Gamma'$ is an unauthorized subset, but U is a maximal unauthorized subset. This is a contradiction. Hence $A \in \Gamma$.

Since $U = A \cup B \notin \Gamma'$ and $A \in \Gamma$, we obtain $B \neq P'$, otherwise $U \in \Gamma'$. Suppose $A \neq P$, and choose any $p \in P \setminus A$. Then $(A \subseteq (U \cup \{p\}) \cap P) \in \Gamma$, and $U \cup \{p\}$ does not contain p'_j , which implies $U \cup \{p\} \notin \Gamma'$. This is a contradiction. Thus $A = P$.

Next, we claim $|P' \setminus B| = 1$.

If $|P' \setminus B| \geq 2$, take any $q \in P' \setminus B$. The set $U \cup \{q\}$ still misses at least one participant in P' , so $U \cup \{q\} \notin \Gamma'$, but U is a maximal unauthorized subset. This is a contradiction. Hence $P' \setminus B$ contains exactly one element p'_j , that is $B = P' \setminus \{p'_j\}$. Combined with $A = P$, we have $U = P \cup (P' \setminus \{p'_j\})$.

It remains to confirm maximality of the two families of sets.

1. For any $R_i \in \mathcal{R}$, since $(R_i \cup P') \cap P = R_i \notin \Gamma$, we have $R_i \cup P' \notin \Gamma'$. Let V satisfy $R_i \cup P' \subsetneq V \subseteq P \cup P'$. Then $R_i \subsetneq V \cap P$. Since R_i is a maximal unauthorized subset in $\mathcal{R}$, $V \cap P \in \Gamma$, so $V \in \Gamma'$. Thus $R_i \cup P'$ is a maximal unauthorized subset in $\mathcal{R}'$.

2. For any $p'_j \in P'$, $P \cup (P' \setminus \{p'_j\}) \notin \Gamma'$ for it does not contain p'_j . Let V satisfy $P \cup (P' \setminus \{p'_j\}) \subsetneq V \subseteq P \cup P'$. Then $p'_j \in V$, so $P' \subseteq V$. Moreover $P \in \Gamma$, $V \cap P = P \in \Gamma$, which implies $V \in \Gamma'$. Therefore $P \cup (P' \setminus \{p'_j\})$ is a maximal unauthorized subset on $P \cup P'$.

Combining all results, the maximal adversary structure of Γ' is

$$\mathcal{R}' = \{R_i \cup P' \mid R_i \in \mathcal{R}\} \cup \{P \cup (P' \setminus \{p'_j\}) \mid p'_j \in P'\}.$$

□

Theorem 5 provides an explicit description for the maximal adversary structure $\mathcal{R}'$ of the access structure Γ' after adding new participants. From this result, we immediately obtain the adversary structure $\mathcal{A}'$, which contains every unauthorized subset.

Corollary 4.1. *Let $\mathcal{A} = 2^P \setminus \Gamma$ be the adversary structure corresponding to the original access structure Γ . Then the adversary structure of new access structure is given by*

$$\mathcal{A}' = \{U \subseteq P \cup P' \mid P' \not\subseteq U \text{ or } U \cap P \in \mathcal{A}\}.$$

Equivalently, $\mathcal{A}' = \{A \cup B \mid A \subseteq P, B \subsetneq P'\} \cup \{A \cup P' \mid A \in \mathcal{A}\}$.

Proof. According to the definition, $U \in \Gamma' \iff P' \subseteq U$ and $U \cap P \in \Gamma$. That is

$$U \notin \Gamma' \iff P' \not\subseteq U \text{ or } U \cap P \notin \Gamma.$$

Since $\mathcal{A} = 2^P \setminus \Gamma$, $U \cap P \notin \Gamma$ is equivalent to $U \cap P \in \mathcal{A}$.

Therefore, $U \in \mathcal{A}' \iff P' \not\subseteq U \text{ or } U \cap P \in \mathcal{A}$, which is the first representation of $\mathcal{A}'$.

Now consider any subset $U \subseteq P \cup P'$. Let $A = U \cap P$ and $B = U \cap P'$, so that $U = A \cup B$ with $A \subseteq P$ and $B \subseteq P'$.

If $P' \not\subseteq U$, then $B \subsetneq P'$, and hence $U = A \cup B$ with $A \subseteq P$ and $B \subsetneq P'$.

If $P' \subseteq U$, then $B = P'$, and $U \cap P \in \mathcal{A}$ implies $A \in \mathcal{A}$. Hence $U = A \cup P'$ with $A \in \mathcal{A}$.

Combining these two cases yields the second equivalent expression for $\mathcal{A}'$.

□

Corollary 4.2. *For any $p'_j \in P'$, if a subset $U \subseteq P \cup P'$ does not contain p'_j , then $U \notin \Gamma'$. Consequently, every new participant in P' is a veto participant of the extended access structure Γ' .*

Proof. If $p'_j \notin U$, then $P' \not\subseteq U$. By the equivalence $U \in \Gamma' \iff P' \subseteq U$ and $U \cap P \in \Gamma$, we obtain $U \notin \Gamma'$. Thus by definition 2.16, each p'_j is a veto participant. □

Corollary 4.3. *Suppose $|\mathcal{R}| = r$ and $|P'| = \ell$, then $|\mathcal{R}'| = r + \ell$.*

Proof. From the theorem 5, we have

$$\mathcal{R}' = \{ R_i \cup P' \mid R_i \in \mathcal{R} \} \cup \{ P \cup (P' \setminus \{p'_j\}) \mid p'_j \in P' \}.$$

The two families are disjoint: the first includes the whole P' , whereas every member of the second misses one element of P' . Their sizes equal r and l respectively, hence $|\mathcal{R}'| = r + l$. $\square$

Corollary 4.4. *Let $|P| = n, |P'| = \ell$. For the extended maximal adversary structure, the cardinality of participants in the first set is $|R_i \cup P'| = |R_i| + \ell$, and the cardinality of participants in the second set is $|P \cup (P' \setminus \{p'_j\})| = n + \ell - 1$.*

In particular, $\max_{R' \in \mathcal{R}'} |R'| = n + \ell - 1$.

Proof. Since $P \cap P' = \emptyset$, in the first set we have $|R_i \cup P'| = |R_i| + \ell$. For the second set, $|P \cup (P' \setminus \{p'_j\})| = |P| + |P'| - 1 = n + \ell - 1$.

As Γ is nonempty and upward closed, and $P \in \Gamma$. It implies that $|R_i| \leq n - 1$, which yields $|R_i \cup P'| \leq n + \ell - 1$.

The second-family reaches this upper bound $n + \ell - 1$, therefore $\max_{R' \in \mathcal{R}'} |R'| = n + \ell - 1$. $\square$

Corollary 4.5. *Given the extended maximal adversary structure $\mathcal{R}'$ and the set of new participants P' , the original maximal adversary structure can be recovered by*

$$\mathcal{R} = \{ R' \cap P \mid R' \in \mathcal{R}', P' \subseteq R' \}.$$

Proof. By Theorem 5, maximal unauthorized subsets in $\mathcal{R}'$ that contain the whole of P' are exactly $R_i \cup P'$ with $R_i \in \mathcal{R}$. Intersecting with P yields $(R_i \cup P') \cap P = R_i$. Meanwhile, every set $P \cup (P' \setminus \{p'_j\})$ cannot contain the full P' and is excluded by the requirement $P' \subseteq R'$. Hence this formula recovers the full collection $\mathcal{R}$. $\square$

Let $\Gamma = \{S_1, S_2, \dots, S_m\}$ be an access structure on the participant set $P = \{p_1, p_2, \dots, p_n\}$, and let $\mathcal{R} = \{R_1, R_2, \dots, R_t\}$ be the corresponding maximal adversary structure. Let

$$P' = \{p'_1, p'_2, \dots, p'_\ell\}, \quad P \cap P' = \emptyset, \quad |P'| = \ell$$

be the set of newly added participants. Define the expanded access structure by

$$\Gamma' = \{S'_1, S'_2, \dots, S'_m\}, \quad S'_i = S_i \cup P', \quad i = 1, 2, \dots, m.$$

We use the following coordinate convention. The 0-th column corresponds to coordinate of the secret; the original participants $p_1, \dots, p_n$ correspond to columns $1, \dots, n$; and the new participants $p'_1, \dots, p'_\ell$ correspond to columns $n + 1, \dots, n + \ell$. Therefore the original matrices have $n + 1$ columns, while the expanded matrices have $n + \ell + 1$ columns.

Let $\mathbb{H}_{m \times (n+1)}$ be the matrix determined by Γ similar to (1). Its i -th row corresponds to S_i , its 0-th column is the all $\mathbf{1}$, and for $1 \leq j \leq n$, the entry $h_{i,j}$ determines whether $p_j \in S_i$. Since

$$S'_i = S_i \cup P',$$

any $p'_j \in S'_i$. Hence the ℓ new columns in the expanded matrix form a block whose entries are all nonzero. This gives the block form following:

$$\mathbb{H}' = (\mathbb{H}_{m \times (n+1)} \quad \mathcal{H}_{m \times \ell}),$$

where $\mathcal{H}_{m \times \ell} = (h_{i,n+j})_{1 \leq i \leq m, 1 \leq j \leq \ell}$, $h_{i,n+j} \neq 0$.

On the other hand, by the preceding result on the change of the maximal adversary structure after adding new participants, the maximal adversary structure corresponding to Γ' is

$$\mathcal{R}' = \{ R_i \cup P' \mid R_i \in \mathcal{R} \} \cup \{ P \cup (P' \setminus \{p'_j\}) \mid p'_j \in P' \}.$$

Order the maximal adversary sets in $\mathcal{R}'$ as $R'_i = R_i \cup P'$, $i = 1, \dots, t$, and $R'_{t+j} = P \cup (P' \setminus \{p'_j\})$, $j = 1, \dots, \ell$.

Let $\mathbb{G}_{t \times (n+1)}$ be the matrix corresponding to $\mathcal{R}$. For the first family of maximal adversary sets, namely $R_i \cup P'$, all newly added participants are contained in the set. Thus the ℓ new coordinate positions are zero, giving the upper right zero block $O_{t \times \ell}$. For the second family, namely $P \cup (P' \setminus \{p'_j\})$, all original participants are contained and exactly one new participant p'_j is missing. Hence the original coordinate part gives the block $\mathcal{G}_1$, whose first column is all 1's and whose remaining entries are zero, while the new coordinate part gives the diagonal block $\mathcal{G}_2$. Therefore the matrix corresponding to $\mathcal{R}'$ has the block form shown :

$$\mathbb{G}' = \begin{pmatrix} \mathbb{G}_{t \times (n+1)} & O_{t \times \ell} \\ \mathcal{G}_1 & \mathcal{G}_2 \end{pmatrix}. \quad (2)$$

More explicitly,

$$\mathcal{G}_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}_{\ell \times (n+1)}, \quad \mathcal{G}_2 = \text{diag}(d_1, d_2, \dots, d_\ell) = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_\ell \end{pmatrix} \quad (3)$$

where $d_j \in \mathbb{F}_q^*$.

We have derived the block structured matrix for the maximal adversary structure after adding new participants. Based on the above matrix characterization, we now present the following lemma for the linear code realization of the expanded access structure.

Lemma 4.1. *Let Γ be an access structure on n participants P , and let $\Gamma' = \{S_i \cup P' \mid S_i \in \Gamma\}$ be the access structure on $P \cup P'$, where $P \cap P' = \emptyset$ and $|P'| = \ell$. Then there exists an $[n+1, k; q]$ linear code $C(n+1)$ realizing Γ if and only if there exists an $[n+\ell+1, k+\ell; q]$ linear code $C(n+\ell+1)$ realizing Γ' .*

Proof. Let $\mathbb{H}_{m \times (n+1)}$ and $\mathbb{G}_{t \times (n+1)}$ be the matrices determined by Γ and $\mathcal{R}$, respectively. Assume that the row space of $\mathbb{G}_{t \times (n+1)}$ is the code $C(n+1)$ and that $\text{rank } \mathbb{G}_{t \times (n+1)} = k$.

By the Theorem 2, the code $C(n+1)$ realizes Γ if and only if

$$\mathbb{H}_{m \times (n+1)} \cdot \mathbb{G}_{t \times (n+1)}^T = 0.$$

We first prove the necessity. Suppose that there exists an $[n+1, k; q]$ linear code $C(n+1)$ realizing Γ , so the above equation holds. Choose arbitrary elements $d_1, d_2, \dots, d_\ell \in \mathbb{F}_q^*$, $\mathcal{G}_2 = \text{diag}(d_1, d_2, \dots, d_\ell)$, and let $\mathcal{G}_1$ be the $\ell \times (n+1)$ matrix in (3) whose first column is all 1's and whose remaining entries are zero. In order to satisfy the matrix equation for the expanded structure, set $h_{i, n+j} = -d_j^{-1}$, $i = 1, 2, \dots, m$, $j = 1, 2, \dots, \ell$.

Then every entry of $\mathcal{H}_{m \times \ell}$ is nonzero, and the j -th column of $\mathcal{H}_{m \times \ell}$ is the constant column $-d_j^{-1}$.

Define

$$\mathbb{H}' = (\mathbb{H}_{m \times (n+1)} \quad \mathcal{H}_{m \times \ell}), \quad \mathbb{G}' = \begin{pmatrix} \mathbb{G}_{t \times (n+1)} & O_{t \times \ell} \\ \mathcal{G}_1 & \mathcal{G}_2 \end{pmatrix}$$

as above. Then $\mathbb{H}'(\mathbb{G}')^T = (\mathbb{H}_{m \times (n+1)} \quad \mathcal{H}_{m \times \ell}) \begin{pmatrix} \mathbb{G}_{t \times (n+1)}^T & \mathcal{G}_1^T \\ O_{t \times \ell}^T & \mathcal{G}_2^T \end{pmatrix}$.

By block matrix multiplication,

$$\mathbb{H}'(\mathbb{G}')^T = (\mathbb{H}_{m \times (n+1)} \mathbb{G}_{t \times (n+1)}^T, \mathbb{H}_{m \times (n+1)} \mathcal{G}_1^T + \mathcal{H}_{m \times \ell} \mathcal{G}_2^T).$$

The first block is zero. For the second block, each row of $\mathcal{G}_1$ is $(1, 0, \dots, 0)$, and the 0-th column of $\mathbb{H}_{m \times (n+1)}$ is the all 1. Hence $\mathbb{H}_{m \times (n+1)} \mathcal{G}_1^T = J_{m \times \ell}$, where $J_{m \times \ell}$ denotes the $m \times \ell$ all 1 matrix.

On the other hand, since $h_{i,n+j} = -d_j^{-1}$, $(\mathcal{H}_{m \times \ell} \mathcal{G}_2^T)_{ij} = h_{i,n+j} d_j = -1$.

Thus $\mathcal{H}_{m \times \ell} \mathcal{G}_2^T = -J_{m \times \ell}$. It follows that $\mathbb{H}_{m \times (n+1)} \mathcal{G}_1^T + \mathcal{H}_{m \times \ell} \mathcal{G}_2^T = 0$, and therefore $\mathbb{H}'(\mathbb{G}')^T = 0$.

By Theorem 2, the row space of $\mathbb{G}'$ realizes Γ' .

It remains to verify the dimension of this row space. Since $\text{rank } \mathbb{G}_{t \times (n+1)} = k$ and $\mathcal{G}_2$ is invertible diagonal, the last ℓ rows of $\mathbb{G}'$ have mutually disjoint nonzero components in the new coordinates. Suppose that

$$\sum_{u=1}^t \alpha_u \mathbf{g}_u + \sum_{v=1}^{\ell} \beta_v \mathbf{g}'_v = 0,$$

where $\mathbf{g}_u$ denotes the row of $\mathbb{G}'$ obtained by appending ℓ zero coordinates to the u -th row of $\mathbb{G}_{t \times (n+1)}$, and $\mathbf{g}'_v$ denotes the $(t+v)$ -th row of $\mathbb{G}'$.

Looking at the last ℓ coordinates gives $\beta_v d_v = 0$ for every v , and hence $\beta_v = 0$ for all v . The remaining part is a linear combination of the rows of $\mathbb{G}_{t \times (n+1)}$, whose row rank is k . Therefore the ℓ newly added rows intersect the original row space trivially and increase the row rank by exactly ℓ . Hence $\text{rank } \mathbb{G}' = k + \ell$.

Therefore the row space of $\mathbb{G}'$ is an $[n + \ell + 1, k + \ell; q]$ linear code $C(n + \ell + 1)$ realizing Γ' .

We now prove the sufficiency. Suppose that there exists an $[n + \ell + 1, k + \ell; q]$ linear code $C(n + \ell + 1)$ realizing Γ' , and that the corresponding matrix is written in the block form of (3) as $\mathbb{G}'$. By Theorem 2, $\mathbb{H}'(\mathbb{G}')^T = 0$. Expanding this equation by blocks, the first t columns give $\mathbb{H}_{m \times (n+1)} \mathbb{G}_{t \times (n+1)}^T = 0$.

Moreover, the last ℓ rows of $\mathbb{G}'$ form an invertible diagonal block on the last ℓ new coordinates, while the first t rows are zero on these coordinates. Thus the row space of $\mathbb{G}'$ is the direct sum of the part generated by the original t rows and the part generated by the last ℓ rows. Consequently, $\text{rank } \mathbb{G}' = \text{rank } \mathbb{G}_{t \times (n+1)} + \ell$.

Because $\text{rank } \mathbb{G}' = k + \ell$, we obtain $\text{rank } \mathbb{G}_{t \times (n+1)} = k$.

Thus the row space of $\mathbb{G}_{t \times (n+1)}$ is an $[n + 1, k; q]$ linear code $C(n + 1)$. Together with $\mathbb{H}_{m \times (n+1)} \mathbb{G}_{t \times (n+1)}^T = 0$, Theorem 2 implies that $C(n + 1)$ realizes the original access structure Γ .

Consequently, an $[n + 1, k; q]$ linear code realizing Γ exists if and only if an $[n + \ell + 1, k + \ell; q]$ linear code realizing Γ' exists. $\square$

After proving the preceding equivalence lemma, we proceed to define the shortening technique over multiple coordinates, which reveals the connection between the code for the expanded access-structure Γ' and the original code.

The lemma 3 and 4 above discuss the shortening operation of a linear code with respect to the last coordinate: one first restricts to the subcode consisting of all codewords whose entry at last coordinate is zero, and then deletes this identically zero coordinate. In order to study the relationship between the access structure obtained after adding several new participants and the original access structure, we need to perform the same operation simultaneously on the coordinates corresponding to the new participants. We keep the notation and the coordinate convention used above.

According to the coordinate convention used above, the 0-th coordinate is the secret, the original participants $p_1, \dots, p_n$ correspond to coordinates $1, \dots, n$, and the new participants $p'_1, \dots, p'_\ell$ correspond to coordinates $n + 1, \dots, n + \ell$. Hence a codeword of $C(n + \ell + 1)$ is written as

$$(c_0, c_1, \dots, c_n, c_{n+1}, \dots, c_{n+\ell}).$$

Let $I = \{n + 1, n + 2, \dots, n + \ell\}$ be the set of coordinates corresponding to the newly added participants.

Define $C(n + \ell + 1)(I) = \{(c_0, c_1, \dots, c_n, 0, \dots, 0) \mid (c_0, c_1, \dots, c_n, 0, \dots, 0) \in C(n + \ell + 1)\}$.

Thus $C(n + \ell + 1)(I)$ is the subcode of $C(n + \ell + 1)$ consisting of all codewords whose last ℓ coordinates are zero. Deleting these zero coordinates gives

$$C(n + \ell + 1)[n + 1] = \{(c_0, c_1, \dots, c_n) \mid (c_0, c_1, \dots, c_n, 0, \dots, 0) \in C(n + \ell + 1)\}.$$

This is the multi coordinate shortening of $C(n + \ell + 1)$ at the coordinate set I . For simplicity, we write

$$C(n + 1) = C(n + \ell + 1)[n + 1].$$

We first construct the expanded generator matrix after adding new participants. From the previous characterization of maximal unauthorized subsets for Γ' , the expanded matrix admits the block structured form

$$\mathbb{G}' = \begin{pmatrix} \mathbb{G}_{t \times (n+1)} & O_{t \times \ell} \\ \mathcal{G}_1 & \mathcal{G}_2 \end{pmatrix},$$

where $O_{t \times \ell}$ denotes the zero matrix,

$$\mathcal{G}_1 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \dots & 0 \end{pmatrix}_{\ell \times (n+1)}, \quad \mathcal{G}_2 = \text{diag}(d_1, d_2, \dots, d_\ell), \quad d_j \in \mathbb{F}_q^*.$$

$\mathcal{G}_2$ is invertible. Let $C(n + \ell + 1) = \text{rowspan}_{\mathbb{F}_q}(\mathbb{G}')$. Define the projection map

$$\psi_I : C(n + \ell + 1) \rightarrow \mathbb{F}_q^\ell, \quad \psi_I(c_0, c_1, \dots, c_{n+\ell}) = (c_{n+1}, \dots, c_{n+\ell}).$$

The image of ψ_I contains the 1 dimensional subspace spanned by rows of $\mathcal{G}_2$. Since the linear independent rows of $\mathcal{G}_2$ lie within the image of ψ_I , its dimension is at least 1, $\text{rank}(\psi_I) = \ell$.

Next compute the dimension of the shortened code. $C(n + \ell + 1)$ is an $[n + \ell + 1, k + \ell; q]$ linear code and $\text{rank } \psi_I = \ell$, then the rank-nullity theorem gives $\dim C(n + \ell + 1)(I) = \dim \ker \psi_I = (k + \ell) - \ell = k$. The projection deleting the last ℓ zero coordinates is injective on $C(n + \ell + 1)(I)$. Therefore $\dim C(n + \ell + 1)[n + 1] = k$.

Indeed, by block matrix multiplication, the second block equation is

$$\mathbb{H}_{m \times (n+1)} \mathcal{G}_1^T + \mathcal{H}_{m \times \ell} \mathcal{G}_2^T = 0.$$

Since the 0-th column of $\mathbb{H}_{m \times (n+1)}$ is the all 1 column and each row of $\mathcal{G}_1$ is $(1, 0, \dots, 0)$, the matrix $\mathbb{H}_{m \times (n+1)} \mathcal{G}_1^T$ is the $m \times \ell$ all 1 matrix. Since $\mathcal{G}_2 = \text{diag}(d_1, \dots, d_\ell)$, the above equation is equal to $1 + h_{i,n+j} d_j = 0$, that is, $h_{i,n+j} = -d_j^{-1}$.

This satisfies the expanded matrix condition and guarantees that the code spanned by $\mathbb{G}'$ realises Γ' .

Lemma 4.2. *Let $C(n + \ell + 1) = \text{rowspan}_{\mathbb{F}_q}(\mathbb{G}')$ be the $[n + \ell + 1, k + \ell; q]$ linear code realizing Γ' , where*

$$\mathbb{G}' = \begin{pmatrix} \mathbb{G}_{t \times (n+1)} & O_{t \times \ell} \\ \mathcal{G}_1 & \mathcal{G}_2 \end{pmatrix}, \quad \text{rank } \mathbb{G}_{t \times (n+1)} = k,$$

and $\mathcal{G}_2$ is invertible. If $C(n + 1) = \{(c_0, c_1, \dots, c_n) \mid (c_0, c_1, \dots, c_n, 0, \dots, 0) \in C(n + \ell + 1)\}$, then $C(n + 1) = \text{rowspan}_{\mathbb{F}_q}(\mathbb{G}_{t \times (n+1)})$, and $C(n + 1)$ is an $[n + 1, k; q]$ linear code realizing Γ .

Proof. Let $c \in C(n + \ell + 1)$. Since $C(n + \ell + 1) = \text{rowspan}_{\mathbb{F}_q}(\mathbb{G}')$, there exist $\mathbf{a} = (a_1, \dots, a_t) \in \mathbb{F}_q^t, \mathbf{b} = (b_1, \dots, b_\ell) \in \mathbb{F}_q^\ell$ such that $\mathbf{c} = (\mathbf{a}, \mathbf{b}) \mathbb{G}'$.

Using the block form of $\mathbb{G}'$, we have $(\mathbf{a}, \mathbf{b}) \mathbb{G}' = (\mathbf{a} \mathbb{G}_{t \times (n+1)} + \mathbf{b} \mathcal{G}_1, \mathbf{b} \mathcal{G}_2)$.

The first component corresponds to the first $n + 1$ coordinates, and the second component corresponds to the last ℓ new participant coordinates.

Suppose now that the last ℓ coordinates of $\mathbf{c}$ are zero. Then $\mathbf{b}\mathcal{G}_2 = 0$. Since $\mathcal{G}_2$ is invertible, it follows that $\mathbf{b} = \mathbf{0}$. Therefore every codeword of $C(n + \ell + 1)$ whose last ℓ coordinates are 0 has the form

$$(\mathbf{a}, 0)\mathbb{G}' = (\mathbf{a}\mathbb{G}_{t \times (n+1)}, 0, \dots, 0), \quad \mathbf{a} \in \mathbb{F}_q^t.$$

After deleting the last ℓ zero coordinates, we obtain $C(n + 1) \subseteq \text{rowspan}_{\mathbb{F}_q}(\mathbb{G}_{t \times (n+1)})$.

For any $\mathbf{x} = \mathbf{a}\mathbb{G}_{t \times (n+1)} \in \text{rowspan}_{\mathbb{F}_q}(\mathbb{G}_{t \times (n+1)})$, we have $(\mathbf{a}, 0)\mathbb{G}' = (\mathbf{x}, 0, \dots, 0) \in C(n + \ell + 1)$. Thus $\mathbf{x} \in C(n + 1)$, and $C(n + 1) = \text{rowspan}_{\mathbb{F}_q}(\mathbb{G}_{t \times (n+1)})$.

Since $\text{rank}(\mathbb{G}_{t \times (n+1)}) = k$, we have $\dim C(n + 1) = k$. Thus $C(n + 1)$ is an $[n + 1, k; q]$ linear code.

It remains to show that $C(n + 1)$ realizes Γ . By the equation blocks $\mathbb{H}'(\mathbb{G}')^T = 0$ implies $\mathbb{H}_{m \times (n+1)}\mathbb{G}_{t \times (n+1)}^T = 0$.

By Theorem 2, the row space of $\mathbb{G}_{t \times (n+1)}$ realizes Γ . Since $C(n + 1) = \text{rowspan}_{\mathbb{F}_q}(\mathbb{G}_{t \times (n+1)})$, the shortened code $C(n + 1)$ realizes Γ . $\square$

4.2 Ideal Secret Sharing Scheme Based on Linear Code

The preceding construction gives a natural correspondence between the original and the expanded linear code realizations through block extension and multi-coordinate shortening. This leads to the following preservation result.

Theorem 4.2. *The access structure Γ can be realized by an ideal linear secret sharing scheme based on a $[n + 1, k; q]$ linear code if and only if the expanded access structure Γ' can be realized by an ideal linear secret sharing scheme based on a $[n + \ell + 1, k + \ell; q]$ linear code.*

Proof. We first prove the necessity. Suppose that Γ can be realized by an ideal linear secret sharing scheme based on a $[n + 1, k; q]$ linear code. Then there exist matrices $\mathbb{H}_{m \times (n+1)}$ and $\mathbb{G}_{t \times (n+1)}$ such that

$$\mathbb{H}_{m \times (n+1)}\mathbb{G}_{t \times (n+1)}^T = 0, \quad \text{rank } \mathbb{G}_{t \times (n+1)} = k.$$

Using the block construction above, take

$$\mathbb{G}' = \begin{pmatrix} \mathbb{G}_{t \times (n+1)} & O_{t \times \ell} \\ \mathcal{G}_1 & \mathcal{G}_2 \end{pmatrix}, \quad \mathcal{G}_2 = \text{diag}(d_1, \dots, d_\ell), \quad d_j \neq 0,$$

and set $h_{i, n+j} = -d_j^{-1}$. As shown in the preceding block matrix, $\mathbb{H}'(\mathbb{G}')^T = 0$.

Therefore $\text{rowspan}_{\mathbb{F}_q}(\mathbb{G}')$ realizes Γ' . Since $\mathcal{G}_2$ is invertible, $\mathbb{G}'$ has rank $k + \ell$. Hence

$$C(n + \ell + 1) = \text{rowspan}_{\mathbb{F}_q}(\mathbb{G}')$$

is an $[n + \ell + 1, k + \ell; q]$ linear code realizing Γ' . In linear secret sharing scheme, the secret and every participant's share are elements of $\mathbb{F}_q$, and hence the scheme is ideal.

We now prove the sufficiency. Suppose that Γ' admits an ideal linear secret sharing scheme realized by an $[n + \ell + 1, k + \ell; q]$ linear code whose generator matrix has the above block form and with $\mathcal{G}_2$ invertible. Shortening this code at the last ℓ new participant coordinates gives

$$C(n + 1) = \{(c_0, c_1, \dots, c_n) \mid (c_0, c_1, \dots, c_n, 0, \dots, 0) \in C(n + \ell + 1)\}.$$

By the shortening technique before, $C(n + 1) = \text{rowspan}_{\mathbb{F}_q}(\mathbb{G}_{t \times (n+1)})$.

Moreover, the first block of $\mathbb{H}'(\mathbb{G}')^T = 0$ yields $\mathbb{H}_{m \times (n+1)}\mathbb{G}_{t \times (n+1)}^T = 0$.

Since $\text{rank}(\mathbb{G}_{t \times (n+1)}) = \text{rank } \mathbb{G}' - \ell = k$, the code $C(n + 1)$ is an $[n + 1, k; q]$ linear code realizing Γ . The corresponding linear secret sharing scheme again has the secret and each participant's share over the same field $\mathbb{F}_q$, and is therefore ideal.

Thus Γ can be realized by an ideal linear secret sharing scheme if and only if Γ' can be realized by an ideal linear secret sharing scheme. $\square$

From Theorem 2, if matrices $\mathbb{H}$ and $\mathbb{G}$ satisfy $\mathbb{G}\mathbb{H}^T = 0$ over $\mathbb{F}_q$, then the linear code generated by the row space of $\mathbb{G}$ can realize the access structure Γ . In the linear secret sharing scheme, the secret s and all participants' shares s_i are on $\mathbb{F}_q$ and the codeword length of the linear code that realizes this access structure is $n + 1$, where n is the number of participants. Hence the linear secret sharing scheme is ideal.

Theorem 4.3. *Let $\Gamma = \{S_1, S_2, \dots, S_m\}$ be a Disjoint Access Structure on the participant set P , that is, $S_i \cap S_j = \emptyset, i \neq j$. Then Γ can be realized by an ideal linear secret sharing scheme.*

Proof. We only consider non-redundant cases, in which every participant is at least in one minimal authorized subset. Since Γ is Disjoint, we have $P = S_1 \dot{\cup} S_2 \dot{\cup} \dots \dot{\cup} S_m$. Let $|S_i| = t_i, i = 1, 2, \dots, m$, then $\sum_{i=1}^m t_i = n$.

We first determine the maximal adversary structure corresponding to Γ by [36]:

$$\mathcal{R} = \{P \setminus \{k_1, k_2, \dots, k_m\} \mid k_i \in S_i, i = 1, 2, \dots, m\}.$$

We now construct the matrices $\mathbb{H}$ and $\mathbb{G}$. For $\mathbb{H}$, choose $h_{i,j} = 1$, if $p_j \in S_i$; $h_{i,j} = 0$, if $p_j \notin S_i$.

Let $T = (k_1, k_2, \dots, k_m) \in S_1 \times S_2 \times \dots \times S_m$. For each T , define the row $\mathbf{g}_T = (g_{T,0}, g_{T,1}, \dots, g_{T,n})$ of $\mathbb{G}$ by $g_{T,0} = 1$, and $g_{T,k_i} = -h_{i,k_i}^{-1} \in \mathbb{F}_q, i = 1, 2, \dots, m$, otherwise is 0. By construction of the maximal adversary structure above, $\mathbb{G}$ is a matrix corresponding to $\mathcal{R}$.

It remains to verify the matrix equation. Let $\mathbf{h}_i$ be the i -th row of $\mathbb{H}$. Since $S_i \cap S_j = \emptyset, i \neq j$, the only participant coordinates where $\mathbf{h}_i$ may be nonzero are those in S_i , and among these coordinates the row $\mathbf{g}_T$ is nonzero only at k_i . Hence

$$\mathbf{h}_i \mathbf{g}_T^T = 1 + h_{i,k_i} g_{T,k_i} = 1 + h_{i,k_i} (-h_{i,k_i}^{-1}) = 0.$$

This holds for $i = 1, 2, \dots, m$ and $T \in S_1 \times \dots \times S_m$ implies $\mathbb{H}\mathbb{G}^T = 0$.

By Theorem 2, the linear code generated by the rows of $\mathbb{G}$ realizes Γ . The secret and each participant's share are elements of $\mathbb{F}_q$. Thus the scheme is ideal, and Γ can be realized by an ideal linear secret sharing scheme. □

To make this construction clearer, we present an example on the field $\mathbb{F}_5$.

Example 4.1. *Let $P = \{p_1, p_2, p_3, p_4, p_5\}$ be the participant set. Define the minimal access structure on P by*

$$\Gamma = \{S_1, S_2\}, \quad S_1 = \{p_1, p_2\}, \quad S_2 = \{p_3, p_4, p_5\}.$$

Since $S_1 \cap S_2 = \emptyset$, the maximal adversary structure is $\mathcal{R} = \{P \setminus \{k_1, k_2\} \mid k_1 \in S_1, k_2 \in S_2\}$. Therefore, $\mathcal{R} = \{\{p_2, p_4, p_5\}, \{p_2, p_3, p_5\}, \{p_2, p_3, p_4\}, \{p_1, p_4, p_5\}, \{p_1, p_3, p_5\}, \{p_1, p_3, p_4\}\}$.

From Theorem 9, the 0-th column of $\mathbb{H}$ is the all 1 column. The entry $h_{i,j}$ is only required to be nonzero whenever $p_j \in S_i$; it is not required to equal 1. Choose

$$h_{1,1} = 2, \quad h_{1,2} = 3, \quad h_{2,3} = 2, \quad h_{2,4} = 3, \quad h_{2,5} = 4.$$

Thus,

$$\mathbb{H} = \begin{pmatrix} 1 & 2 & 3 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 3 & 4 \end{pmatrix}.$$

In $\mathbb{F}_5$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$. It follows that $-2^{-1} = 2$, $-3^{-1} = 3$, $-4^{-1} = 1$.

For every $T = (k_1, k_2) \in S_1 \times S_2$, define a row $\mathbf{g}_T = (g_{T,0}, g_{T,1}, \dots, g_{T,5})$ of $\mathbb{G}$, as in the construction in Theorem 9, by $g_{T,0} = 1, g_{T,k_i} = -h_{i,k_i}^{-1}, i = 1, 2$. Thus,

$$\mathbb{G} = \begin{pmatrix} 1 & 2 & 0 & 2 & 0 & 0 \\ 1 & 2 & 0 & 0 & 3 & 0 \\ 1 & 2 & 0 & 0 & 0 & 1 \\ 1 & 0 & 3 & 2 & 0 & 0 \\ 1 & 0 & 3 & 0 & 3 & 0 \\ 1 & 0 & 3 & 0 & 0 & 1 \end{pmatrix}.$$

We now describe the correspondence between $\mathbb{G}$ and $\mathcal{R}$. For the first row $\mathbf{g}_{(p_1, p_3)} = (1, 2, 0, 2, 0, 0)$, the zero participant coordinates are p_2, p_4, p_5 . These are precisely the participants in the maximal unauthorized set $P \setminus \{p_1, p_3\} = \{p_2, p_4, p_5\}$. Similarly, the zero participant coordinates of every row $\mathbf{g}_T$ are exactly the elements of the maximal unauthorized subset $P \setminus \{k_1, k_2\}$. Hence $\mathbb{G}$ is the matrix corresponding to $\mathcal{R}$.

In fact, $\text{rank}(\mathbb{H}) = 2, \text{rank}(\mathbb{G}) = 4$. Since $\mathbb{H}\mathbb{G}^T = 0$, $\text{rowspan}_{\mathbb{F}_5}(\mathbb{G}) \subseteq \ker(\mathbb{H})$. By the rank-nullity theorem, $\dim_{\mathbb{F}_5} \ker(\mathbb{H}) = 6 - \text{rank}(\mathbb{H}) = 4$. It follows that $\text{rowspan}_{\mathbb{F}_5}(\mathbb{G}) = \ker(\mathbb{H})$.

The resulting linear code can be written as

$$C = \{(s, x_1, x_2, x_3, x_4, x_5) \in \mathbb{F}_5^6 \mid s + 2x_1 + 3x_2 = 0, s + 2x_3 + 3x_4 + 4x_5 = 0\}.$$

In other words, $s = 3x_1 + 2x_2 = 3x_3 + 2x_4 + x_5$.

In the following, we present an ideal linear secret sharing scheme for the above access structure.

Let the secret be $s \in \mathbb{F}_5$. The dealer independently and uniformly chooses $r, a, b \in \mathbb{F}_5$ and distributes the following shares:

Participant	p_1	p_2	p_3	p_4	p_5
Share	r	$3s + r$	a	b	$s - 3a - 2b$

That is, $x_1 = r, x_2 = 3s + r, x_3 = a, x_4 = b, x_5 = s - 3a - 2b$.

These shares indeed define a codeword of C . Since $6s = s$ and $5r = 0$ in $\mathbb{F}_5$, $3x_1 + 2x_2 = 3r + 2(3s + r) = 3r + 6s + 2r = s$.

Similarly, $3x_3 + 2x_4 + x_5 = 3a + 2b + (s - 3a - 2b) = s$. Thus, $(s, x_1, x_2, x_3, x_4, x_5) \in C$.

Every authorized set can reconstruct the secret. If an authorized set contains $S_1 = \{p_1, p_2\}$, then it computes

$$s = 3x_1 + 2x_2.$$

If it contains $S_2 = \{p_3, p_4, p_5\}$, then it computes $s = 3x_3 + 2x_4 + x_5$. Therefore, every set containing S_1 or S_2 can recover s .

We now prove perfect privacy for unauthorized sets. Since every unauthorized set is contained in a maximal unauthorized set, it suffices to consider

$$R = P \setminus \{k_1, k_2\}, \quad k_1 \in S_1, \quad k_2 \in S_2.$$

The set R observes at most one of x_1, x_2 . Since r is uniformly distributed over $\mathbb{F}_5$, $x_1 = r$ is uniform; similarly, $x_2 = 3s + r$ is uniform with a distribution independent of s . Thus the shares in the S_1 component reveal no information about s .

Similarly, R observes at most two of x_3, x_4, x_5 . Because (a, b) is uniformly distributed over $\mathbb{F}_5^2$, every pair of these three shares has a joint distribution independent of s . Hence the shares in the S_2 component also reveal no information about s .

The randomness r used for the S_1 component is independent of the randomness a, b used for the S_2 component. Accordingly, the joint distribution of all shares held by any maximal unauthorized set is independent of the secret s . The scheme is therefore perfectly secure.

Furthermore, the secret s and every participant's share are elements of the same finite field $\mathbb{F}_5$, so every share has the same size as the secret. In addition, all shares are linear functions of s, r, a, b . Hence this is an ideal linear secret sharing scheme realizing Γ . $\square$

Corollary 4.6. Let $\Gamma = \{S_1, S_2\}$ be a minimal access structure on the participant set P ; that is, the number of minimal authorized subsets of Γ is 2. Then Γ can be realized by an ideal linear secret sharing scheme.

Proof. If $S_1 \cap S_2 = \emptyset$, then Γ is a Disjoint Access Structure, it follows trivially from Theorem 9.

Now assume that $D = S_1 \cap S_2 \neq \emptyset$. Since S_1 and S_2 are both minimal authorized subsets, neither is contained in the other. Hence $S_1 \setminus D \neq \emptyset, S_2 \setminus D \neq \emptyset$.

Let $P_0 = (S_1 \setminus D) \cup (S_2 \setminus D) = P \setminus D$. Define the minimal access structure on P_0 by $\Gamma_0 = \{S_1 \setminus D, S_2 \setminus D\}$.

Then $(S_1 \setminus D) \cap (S_2 \setminus D) = \emptyset$, so Γ_0 is a Disjoint access structure. By Theorem 9, Γ_0 admits an ideal linear secret sharing realization.

On the other hand, $D \cap P_0 = \emptyset$, and the original participant set satisfies $P = P_0 \cup D$. The original access structure Γ is obtained from Γ_0 by adding the participant set D to every minimal authorized subset:

$$\Gamma = \{(S_1 \setminus D) \cup D, (S_2 \setminus D) \cup D\}.$$

This is similar to the Theorem 5, with original participant set P_0 , newly added participant set D , and expanded minimal authorized subsets obtained by adding D to each member of Γ_0 . Theorem 8 guarantees that Γ can be realized by an ideal linear secret sharing scheme. $\square$

The corollary establishes that every minimal access structure containing exactly two minimal authorized subsets admits an ideal linear secret sharing realization. Next, we rely on the classification of two classic families of maximal cliques in Johnson graphs, namely star cliques and top cliques[37], and present a lemma characterizing the bipartite structure of such families of sets.

Lemma 4.3. *Let $\mathcal{F} = \{S_1, \dots, S_m\}$ be a collection of distinct t element subsets with $m \geq 2$. Suppose that*

$$|S_i \cap S_j| = t - 1, \quad 1 \leq i < j \leq m.$$

Then $\mathcal{F}$ is of one of the following two forms:

1. **Star type:** *There exists a $(t - 1)$ -subset B such that every S_i has the form*

$$S_i = B \cup \{x_i\},$$

where $x_1, \dots, x_m$ are pairwise distinct;

2. **Top type:** *There exists a $(t + 1)$ -subset U such that*

$$S_i \subseteq U, \quad |S_i| = t,$$

for every i . In addition:

when $m = 2$, $\mathcal{F}$ may satisfy both definitions;

when $m \geq 3$, $\mathcal{F}$ must be either Star type or Top type.

Proof. For two distinct sets S_1, S_2 . Let $B = S_1 \cap S_2, S_1 = B \cup \{x\}, S_2 = B \cup \{y\}$, where $|B| = t - 1$ and $x \neq y$.

Case 1: $m = 2$.

The collection is $\mathcal{F} = \{S_1, S_2\}$. And $S_1 = B \cup \{x\}, S_2 = B \cup \{y\}$, $\mathcal{F}$ is Star type.

Define $U = S_1 \cup S_2, |U| = |B \cup \{x, y\}| = (t - 1) + 2 = t + 1$. We have $S_1 \subseteq U, S_2 \subseteq U$, so $\mathcal{F}$ also satisfies top type.

Therefore for $m = 2$, the collection is both types, and the lemma statement holds.

Case 2: Consider any S_r with $r \geq 3$.

If $B \subseteq S_r$, then $|S_r| = t$ implies $S_r = B \cup \{z_r\}$ for some element z_r .

If $B \not\subseteq S_r$, S_r misses exactly one element of B . Otherwise, $|S_r \cap S_1| \leq t - 2$, contradicting the hypothesis. Let $b \in B \setminus S_r$.

Since $|S_r \cap S_1| = |S_r \cap S_2| = t - 1$, S_r must contain both x and y . Therefore,

$$S_r = (B \setminus \{b\}) \cup \{x, y\} \subseteq U, \quad U = B \cup \{x, y\}.$$

Now we prove that Star type and Top type subsets cannot both appear within $\mathcal{F}$ for $m \geq 3$. Suppose that there exist a Star type set $B \cup \{z\}$ different from S_1, S_2 with $z \notin \{x, y\}$, and a Top type set $(B \setminus \{b\}) \cup \{x, y\}$. Their intersection is at most $t - 2$, contradicting the pairwise intersection assumption. It follows that all subsets of $\mathcal{F}$ must be a Star type or a Top type for $m \geq 3$. $\square$

The above lemma categorises every family satisfying the corresponding constraints as either Star type or Top type. In the following theorem, we focus on the minimal access structures satisfying the pairwise intersection condition, and derive their maximal adversary structures for both types.

Theorem 4.4. *Let $\Gamma = \{S_1, S_2, \dots, S_m\}$ be an access structure on the participant set P , where $m \geq 2$. Suppose that $|S_i \cap S_j| = |S_i| - 1 = |S_j| - 1$ for $i \neq j$ and $|S_i| = t$. By Lemma 10, Γ is of Star type or Top type, and its maximal adversary structure is as follows:*

1. *If $\Gamma = \{S_i = B \cup \{x_i\} | i = 1, \dots, m\}$ is the Star type, and the corresponding maximal adversary structure is*

$$\mathcal{R} = \{P \setminus \{b_\ell\} | b_\ell \in B\} \cup \{B\}.$$

2. *If $\Gamma = \{P \setminus \{p_i\} : i \in M\}$ is the Top type, then $P = U$, $n = t + 1$ and there exists an index set $M \subseteq [n]$, with $|M| = m$. Then the corresponding maximal adversary structure is*

$$\mathcal{R} = \{P \setminus \{p_j\} | j \notin M\} \cup \{P \setminus \{p_i, p_j\} | i, j \in M, i < j\}.$$

Proof. First consider the Star type case. A subset is authorized if and only if it contains the whole common core B and at least one of the elements x_i . Hence an unauthorized set is of one of two types: those omitting some $b_\ell \in B$, and those containing B but none of the x_i .

If an unauthorized set excludes b_ℓ , then it is in $P \setminus \{b_\ell\}$. The set $P \setminus \{b_\ell\}$ is an unauthorized set, and its only proper superset is P , which is authorized. Hence $P \setminus \{b_\ell\}$ is a maximal unauthorized set. If an unauthorized set contains B but no x_i , then it is in B . The set B is an unauthorized set, and adding any x_i is the minimal authorized set $B \cup \{x_i\}$. Hence B is the maximal unauthorized set. This proves that, in the Star type case,

$$\mathcal{R} = \{P \setminus \{b_\ell\} | b_\ell \in B\} \cup \{B\}.$$

Now consider the Top type case. A subset is an authorized set if and only if it contains $P \setminus \{p_i\}$ for some $i \in M$. Let $A \subseteq P$ be an unauthorized set, and set $D = P \setminus A$. If $|D| = 1$ and $D = \{p_i\}$ for some $i \in M$, then $A = P \setminus \{p_i\}$ is a minimal authorized set, a contradiction. Thus a missing set of size one gives an unauthorized subset only when $D = \{p_j\}$ with $j \notin M$. In this case $A = P \setminus \{p_j\}$, and its only proper superset is P , so it is a maximal unauthorized set.

If $|D| = 2$, there are three possibilities.

If D contains some p_j with $j \notin M$, then adding the other missing participant still leaves the unauthorized set $P \setminus \{p_j\}$, so A is not maximal unauthorized set.

If $D = \{p_i, p_j\}$ with $i, j \in M$, then $A = P \setminus \{p_i, p_j\}$ is an unauthorized set, while adding p_i or p_j is $P \setminus \{p_j\}$ or $P \setminus \{p_i\}$, respectively, both of which are minimal authorized sets. Hence A is maximal unauthorized set.

If $|D| \geq 3$, adding one missing participant still leaves at least two participants absent; the set is still an unauthorized set. Therefore such an A cannot be maximal unauthorized set. The stated description of $\mathcal{R}$ follows:

$$\mathcal{R} = \{P \setminus \{p_j\} | j \notin M\} \cup \{P \setminus \{p_i, p_j\} | i, j \in M, i < j\}.$$

$\square$

Theorem 4.5. Let $\Gamma = \{S_1, S_2, \dots, S_m\}$ be a minimal access structure on n participant set P . Suppose $|S_i \cap S_j| = |S_i| - 1 = |S_j| - 1$ for $i \neq j, i, j \in \{1, \dots, m\}$, then there exists an ideal linear secret sharing scheme realizing Γ over the finite field $\mathbb{F}_q$, $q \geq m$.

Proof. For $m = 1$, the statement holds trivially.

If $m \geq 2$. The hypopaper implies that all S_i have the same cardinality, that is, $|S_i| = t$, $i = 1, \dots, m$.

By the Lemma 10, Γ is of Star type or Top type. By Theorem 11, the corresponding maximal structure $\mathcal{R}$ is already determined. It remains only to construct matrices satisfying $\mathbb{H}\mathbb{G}^T = 0$.

Case 1: Γ is of Star type.

Suppose that $S_i = B \cup \{x_i\}, i = 1, \dots, m$, where $B = \{b_1, \dots, b_{t-1}\}, P = B \cup \{x_1, \dots, x_m\}$.

By the Theorem 11, the corresponding maximal structure is

$$\mathcal{R} = \{P \setminus \{b_\ell\} : 1 \leq \ell \leq t-1\} \cup \{B\}.$$

Choose arbitrary nonzero elements $a_\ell, c_i \in \mathbb{F}_q^*$ for $1 \leq \ell \leq t-1, 1 \leq i \leq m$. Construct $\mathbb{H}$ with row i corresponding to S_i by setting $h_{i,0} = 1, h_{i,b_\ell} = a_\ell, h_{i,x_i} = c_i, h_{i,x_j} = 0$ where $j \neq i$.

For $\mathbb{G}$, let $\mathbf{g}^{(\ell)}$ correspond to $P \setminus \{b_\ell\}$ and set $g_0^{(\ell)} = 1, g_{b_\ell}^{(\ell)} = -a_\ell^{-1}$, with all other participant coordinates equal to 0. Let $\mathbf{g}^{(B)}$ correspond to B and set $g_0^{(B)} = 1, g_{x_i}^{(B)} = -c_i^{-1}$, with all other participant coordinates equal to 0.

Then, for every i, ℓ , $\mathbf{h}_i(\mathbf{g}^{(\ell)})^T = 1 + a_\ell(-a_\ell^{-1}) = 0, \mathbf{h}_i(\mathbf{g}^{(B)})^T = 1 + c_i(-c_i^{-1}) = 0$.

Hence $\mathbb{H}\mathbb{G}^T = 0$. By the Theorem 2, there exists an ideal linear secret sharing scheme to realize Γ on $\mathbb{F}_q$.

Case 2: Γ is of Top type.

Suppose that $\Gamma_{\min} = \{P \setminus \{p_i\} | i \in M\}, |M| = m$, and the corresponding maximal structure is

$$\mathcal{R} = \{P \setminus \{p_j\} | j \notin M\} \cup \{P \setminus \{p_i, p_j\} | i, j \in M, i < j\}.$$

Choose pairwise distinct $\alpha_i \in \mathbb{F}_q$ for $i \in M$, which is possible when $q \geq m$, and choose an arbitrary $\beta \in \mathbb{F}_q^*$. Construct row r of $\mathbb{H}$ by associating it with $P \setminus \{p_r\}$ and setting

$$h_{r,0} = 1, h_{r,r} = 0, h_{r,i} = \alpha_i - \alpha_r (i \in M, i \neq r), h_{r,j} = \beta (j \notin M).$$

Thus the only zero participant coordinate in row r is p_r .

Now construct $\mathbb{G}$. If $j \notin M$, let $\mathbf{g}^{(j)}$ correspond to $P \setminus \{p_j\}$ and set $g_0^{(j)} = 1, g_j^{(j)} = -\beta^{-1}$, with all other participant coordinates equal to 0.

If $i < j$ and $i, j \in M$, let $\delta_{ij} = \alpha_j - \alpha_i \neq 0$, and let $\mathbf{g}^{(i,j)}$ correspond to $P \setminus \{p_i, p_j\}$ with

$$g_0^{(i,j)} = 1, g_i^{(i,j)} = \delta_{ij}^{-1}, g_j^{(i,j)} = -\delta_{ij}^{-1},$$

and all other participant coordinates equal to 0.

The orthogonality checks are immediate:

$$\mathbf{h}_r(\mathbf{g}^{(j)})^T = 1 + \beta(-\beta^{-1}) = 0 \quad (j \notin M, r \in M),$$

and for $i < j$ in M ,

$$\mathbf{h}_i(\mathbf{g}^{(i,j)})^T = 1 + (\alpha_j - \alpha_i)(-\delta_{ij}^{-1}) = 0,$$

$$\mathbf{h}_j(\mathbf{g}^{(i,j)})^T = 1 + (\alpha_i - \alpha_j)\delta_{ij}^{-1} = 0,$$

$$\mathbf{h}_r(\mathbf{g}^{(i,j)})^T = 1 + (\alpha_i - \alpha_r)\delta_{ij}^{-1} - (\alpha_j - \alpha_r)\delta_{ij}^{-1} = 1 + (\alpha_i - \alpha_j)\delta_{ij}^{-1} = 0 \quad (r \in M \setminus \{i, j\}).$$

Therefore $\mathbb{H}\mathbb{G}^T = 0$. By the Theorem 2, there exists an ideal linear secret sharing scheme to realize Γ on $\mathbb{F}_q$. $\square$

Corollary 4.7. *Let Γ be the $(n-1, n)$ -threshold access structure. Let $\Gamma_M \subsetneq \Gamma$ with $2 \leq |\Gamma_M| \leq n-1$. Then Γ_M can be realized by an ideal linear secret sharing scheme.*

Proof. Let $M \subseteq [n]$ with $2 \leq |M| \leq n-1$, and define

$$\Gamma_M = \{P \setminus \{p_i\} | i \in M\}.$$

For any distinct $i, j \in M$,

$$|(P \setminus \{p_i\}) \cap (P \setminus \{p_j\})| = n-2 = |P \setminus \{p_i\}| - 1.$$

Thus Γ_M satisfies Theorem 12, so it can be realized by an ideal linear secret sharing scheme. $\square$

In Theorem 5, we considered the maximal adversary structure obtained by adding the new participants to every minimal authorized subset. To investigate more dynamic scenarios with newly added participants, we study the access structure induced by adding new participants only to only part of minimal authorized subsets. We first characterize its corresponding maximal adversary structure together with the required notation. Explicit formulas for such characterization are presented in the theorem below.

Let P be the original participant set, and Γ be an access structure on P with minimal authorized

$$\Gamma_{\min} = \{S_i | i \in [m]\}.$$

Let $\mathcal{R}$ be the maximal adversary structure corresponding to Γ and Q be a nonempty set of new participants such that $P \cap Q = \emptyset$.

Choose $J \subseteq [m]$. Define the expanded access structure $\hat{\Gamma}$ by $\hat{\Gamma}_{\min} = \{S_i \cup Q | i \in J\} \cup \{S_i | i \notin J\}$. Thus only the minimal authorized subsets indexed by J are enlarged by Q .

For convenience, define the auxiliary access structure Γ_0 generated by the minimal authorized subsets S_i for $i \notin J$ that are not expanded. If $J = [m]$, then Γ_0 has no minimal authorized subset, and we set $\mathcal{R}_0 = \{P\}$.

In general, let $\mathcal{R}_0$ be the maximal adversary structure corresponding to Γ_0 , and define $\mathcal{R}_1 = \{T \in \mathcal{R}_0 | \exists i \in J, S_i \subseteq T\}$.

Thus $\mathcal{R}_1$ consists of those members of $\mathcal{R}_0$ that contain at least one minimal authorized subset whose index is in J .

Theorem 4.6. *Let $\hat{\Gamma}_{\min} = \{S_i \cup Q | i \in J\} \cup \{S_i | i \notin J\}$, then the corresponding maximal adversary structure is*

$$\hat{\mathcal{R}} = \{R \cup Q | R \in \mathcal{R}\} \cup \{T \cup (Q \setminus \{q\}) | T \in \mathcal{R}_1, q \in Q\}.$$

Proof. If $Q = \{q\}$, the maximal adversary structure reduces to $\hat{\mathcal{R}} = \{R \cup \{q\} | R \in \mathcal{R}\} \cup \mathcal{R}_1$.

If only one minimal authorized subset S_r is expanded, namely $J = \{r\}$, then $\mathcal{R}_1 = \{T \in \mathcal{R}_0 | S_r \subseteq T\}$.

For $U \subseteq P \cup Q$, let $U_P = U \cap P, U_Q = U \cap Q$. Therefore, U is an authorized set in $\hat{\Gamma}$ if and only if either $U_P \in \Gamma_0$, or $Q \subseteq U_Q$ and $\exists i \in J$ such that $S_i \subseteq U_P$.

If $U_Q = Q$, then U is an unauthorized set if and only if U_P is an unauthorized set in the original access structure Γ . Hence the maximal unauthorized sets of this type are exactly

$$R \cup Q, R \in \mathcal{R}.$$

Now suppose $U_Q \neq Q$. Then U cannot contain any set $S_i \cup Q$. We force on the maximal unauthorized subset, thus U contains all but one new participant, so $U_Q = Q \setminus \{q\}$ for some $q \in Q$. Moreover, U_P must be a maximal unauthorized set corresponding to Γ_0 , that is, $U_P \in \mathcal{R}_0$.

Finally, after adding the only missing new participant q , the resulting set must become an authorized subset; equivalently, U_P must contain some S_i with $i \in J$. Thus $U_P \in \mathcal{R}_1$. The maximal unauthorized subsets of this type are therefore

$$T \cup (Q \setminus \{q\}), T \in \mathcal{R}_1, q \in Q.$$

□

To better demonstrate the Theorem above, we provide a specific example in follows.

Example 4.2. Let participants be $P = \{1, 2, 3, 4, 5\}$. Consider the access structure Γ on P whose minimal access structure is

$$\Gamma_{\min} = \{S_1, S_2, S_3\} = \{\{1, 2\}, \{2, 3\}, \{4, 5\}\}.$$

The corresponding maximal adversary structure of Γ is $\mathcal{R} = \{\{2, 4\}, \{2, 5\}, \{1, 3, 4\}, \{1, 3, 5\}\}$.

Let the new participant set be $Q = \{6, 7\}$. We expand only $S_1 = \{1, 2\}$, that is, $J = \{1\}$. The expanded minimal access structure $\hat{\Gamma}$ is

$$\hat{\Gamma}_{\min} = \{\{1, 2, 6, 7\}, \{2, 3\}, \{4, 5\}\}.$$

The minimal authorized subsets that are not expanded are $S_2 = \{2, 3\}, S_3 = \{4, 5\}$. Thus the auxiliary access structure Γ_0 is generated by $S_2 = \{2, 3\}, S_3 = \{4, 5\}$.

A subset is an unauthorized subset corresponding to Γ_0 if and only if it contains neither $\{2, 3\}$ nor $\{4, 5\}$. Therefore

$$\mathcal{R}_0 = \{\{1, 2, 4\}, \{1, 2, 5\}, \{1, 3, 4\}, \{1, 3, 5\}\}.$$

By definition above, $\mathcal{R}_1 = \{T \in \mathcal{R}_0 | S_1 \subseteq T\}$. Since $S_1 = \{1, 2\}$, we have

$$\mathcal{R}_1 = \{\{1, 2, 4\}, \{1, 2, 5\}\}.$$

By Theorem 13, $\hat{\mathcal{R}} = \{R \cup Q | R \in \mathcal{R}\} \cup \{T \cup (Q \setminus \{q\}) | T \in \mathcal{R}_1, q \in Q\}$.

The first family is $\{R \cup Q | R \in \mathcal{R}\} = \{\{2, 4, 6, 7\}, \{2, 5, 6, 7\}, \{1, 3, 4, 6, 7\}, \{1, 3, 5, 6, 7\}\}$. The second family is $\{T \cup (Q \setminus \{q\}) | T \in \mathcal{R}_1, q \in Q\} = \{\{1, 2, 4, 6\}, \{1, 2, 4, 7\}, \{1, 2, 5, 6\}, \{1, 2, 5, 7\}\}$. Thus the maximal adversary structure of the expanded access structure is

$$\begin{aligned} \hat{\mathcal{R}} = \{ & \{2, 4, 6, 7\}, \{2, 5, 6, 7\}, \{1, 3, 4, 6, 7\}, \{1, 3, 5, 6, 7\}, \\ & \{1, 2, 4, 6\}, \{1, 2, 4, 7\}, \{1, 2, 5, 6\}, \{1, 2, 5, 7\} \}. \end{aligned}$$

□

5 Conclusion

This paper studied ideal linear secret sharing schemes under participant updates. We characterized the changes of maximal adversary structures when new participants are added either to all authorized subsets or only to a part of minimal authorized subsets. We also establish equivalence conditions for constructing the original and expanded access structures from linear codes, and demonstrate that the optimal information rate property is maintained via the corresponding block-matrix construction and code shortening operation. Furthermore, we prove that several classes of access structures can be realized by ideal linear secret sharing schemes. These families include Disjoint Access Structures, as well as Star type and Top type structures derived from minimal authorized subsets that differ by only one participant pairwise. These results establish a complete analytical perspective for analyzing access structures, maximal adversary structures, and the optimal information rate under dynamic participant settings.

References

- [1] Y. Ma, Q. Cheng, Z. Liu, X. Luo, and X. Chen. 2PCLGA: Privacy-preserving and provable-secure certificateless group key agreement scheme for the distributed learning-based MEC networks. *IEEE Transactions on Dependable and Secure Computing*, 23(2):3119–3130, 2026. doi: 10.1109/TDSC.2025.3632556.
- [2] Y. Rajkumar and S. V. N. S. Kumar. A dickson polynomial based group key agreement authentication scheme for ensuring conditional privacy preservation and traceability in VANETs. *Scientific Reports*, 15(1):6211, 2025. doi: 10.1038/s41598-025-89208-5.
- [3] Z. Wang, J. Zhang, Y. Tang, and H. Cheng. BGAS: Blockchain-based secure and efficient group key agreement scheme for dynamic vehicular platoon. *Cluster Computing*, 28(1):59, 2025. doi: 10.1007/s10586-024-04784-x.
- [4] A. Kumar, B. Sharma, and A. Noonia. Secure blockchain based intrusion detection for IoT networks. *Distributed Computing*, 28(1):226, 2025. doi: 10.1007/s10791-025-09754-4.
- [5] Y. Wu, X. Wang, W. Susilo, G. Yang, Z. L. Jiang, J. Li, and X. Liu. Mixed-protocol multi-party computation framework towards complex computation tasks with malicious security. *Computer Standards & Interfaces*, 80:103570, 2022. doi: 10.1016/j.csi.2021.103570.
- [6] Y. Xu, Z. Peng, C. Zhang, G. Wang, H. Wang, H. Jiang, and Y. Zhang. Enhancing privacy in cyber-physical systems: An efficient blockchain-assisted data-sharing scheme with deniability. *Journal of Systems Architecture*, 150:103132, 2024. doi: 10.1016/j.sysarc.2024.103132.
- [7] S. Feng and L. F. Zhang. An efficient method for realizing contractions of access structures in cloud storage. *IEEE Transactions on Services Computing*, 16(6):4481–4492, 2023. doi: 10.1109/TSC.2023.3325894.
- [8] K. Gai, D. Wang, J. Yu, L. Zhu, and W. Meng. A scheme of robust privacy-preserving multi-party computation via public verification. *IEEE Transactions on Dependable and Secure Computing*, 22(5):4896–4910, 2025. doi: 10.1109/TDSC.2025.3555284.
- [9] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
- [10] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the International Workshop on Managing Requirements Knowledge*, pages 313–313. IEEE Computer Society, 1979.
- [11] A. Beimel. *Secure schemes for secret sharing and key distribution*. PhD thesis, Technion—Israel Institute of Technology, 1996.
- [12] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology—CRYPTO’90*, volume 537 of *Lecture Notes in Computer Science*, pages 27–35. Springer, 1990.
- [13] C. Blundo, A. De Santis, and D. R. Stinson. Graph decompositions and secret sharing schemes. *Journal of Cryptology*, 8(1):39–64, 1995.
- [14] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.
- [15] L. Xiao and M. Liu. Linear secret sharing schemes and rearrangements of access structures. *Acta Mathematicae Applicatae Sinica*, 20(4):685–694, 2004.

- [16] Z. Guan, Z. Wan, Y. Yang, Y. Zhou, and B. Huang. BlockMaze: An efficient privacy-preserving account-model blockchain based on zk-SNARKs. *IEEE Transactions on Dependable and Secure Computing*, 19(3):1446–1463, 2022. doi: 10.1109/TDSC.2020.3025129.
- [17] C. Xu, P. Zhang, H. Yu, and Y. Li. Dynamic blockchain-empowered trustworthy end-edge collaborative computing via rotating multi-agent DRL. *IEEE Transactions on Wireless Communications*, 24(6):4864–4878, 2025. doi: 10.1109/TWC.2025.3544478.
- [18] D. Zhang, J. Le, X. Lei, T. Xiang, and X. Liao. Secure redactable blockchain with dynamic support. *IEEE Transactions on Dependable and Secure Computing*, 21(2):717–731, 2024. doi: 10.1109/TDSC.2023.3261343.
- [19] Z. Zhang, B. Hu, H. Chen, Y. Zhou, H. Jiang, and J. Liu. DyCAPS: Asynchronous dynamic-committee proactive secret sharing. *Chinese Journal of Electronics*, 35(1):307–321, 2026. doi: 10.23919/cje.2025.00.072.
- [20] L. Alvisi, D. Malkhi, E. Pierce, M. K. Reiter, and R. N. Wright. Dynamic byzantine quorum systems. In *Proceedings International Conference on Dependable Systems and Networks. DSN 2000*, pages 283–292. IEEE, 2000.
- [21] R. Eriguchi, N. Kunihiro, and K. Nuida. Multiplicative and verifiably multiplicative secret sharing for multipartite adversary structures. *Designs, Codes and Cryptography*, 91(5):1751–1778, 2023. doi: 10.1007/s10623-022-01177-2.
- [22] H. Qin, Y. Dai, and Z. Wang. A secret sharing scheme based on (t, n) threshold and adversary structure. *International Journal of Information Security*, 8(5):379–385, 2009.
- [23] T. Wu, S. Zhu, F. Li, and L. Liu. Two quantum secret sharing schemes with adversary structure. *International Journal of Theoretical Physics*, 61(7), 2022. doi: 10.1007/s10773-022-05176-w.
- [24] M. Bertilsson and I. Ingemarson. A construction of practical secret sharing schemes using linear block codes. In *Theory and Application of Cryptographic Techniques*, volume 658 of *Lecture Notes in Computer Science*, pages 67–79. Springer, 1992.
- [25] J. Martí-Farré and C. Padró. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. *Designs, Codes and Cryptography*, 52(1):1–14, 2009.
- [26] J. Yuan and C. Ding. Secret sharing schemes from three classes of linear codes. *IEEE Transactions on Information Theory*, 52(1):206–212, 2006.
- [27] R. J. McEliece and D. V. Sarwate. On sharing secrets and reed-solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.
- [28] J. L. Massey. Minimal codewords and secret sharing. In *Proc. 6th Swedish-Russian Int. Workshop Inf. Theory*, pages 246–249, 1993.
- [29] C. Tang, S. Gao, and C. Zhang. The optimal linear secret sharing scheme for any given access structure. *Journal of Systems Science & Complexity*, 26(4):634–649, 2013.
- [30] T. 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.
- [31] 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.

- [32] C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory*, 46:2596–2605, 2000.
- [33] J. Martí-Farré and C. Padró. Secret sharing schemes with three or four minimal qualified subsets. *Designs, Codes and Cryptography*, 34(1):17–34, 2005.
- [34] C. Ding and A. Salomaa. Secret sharing schemes with nice access structures. *Fundamenta Informaticae*, 73(1/2):51–62, 2006.
- [35] Y. Song, Z. Li, and Y. Li. Secret sharing schemes based on minimal linear codes. *Acta Electronica Sinica*, 41(2):220–226, 2013.
- [36] C. Tang, Q. Xu, and G. Hu. Finding the maximal adversary structure from any given access structure. *Information Sciences*, 508:329–342, 2020. doi: 10.1016/j.ins.2019.08.057.
- [37] P. Shuldiner and W. Oldford. Clique types in johnson graphs, 2020. arXiv preprint.