Quantum Secret Sharing Scheme on Hypercyclic Quantum Structures

Lei Li, Zhi Li.

Abstract

This paper investigates the construction of efficient quantum secret sharing schemes for quantum access structures based on hypergraphs with three hyperedges. We prove that hypercycles with three hyperedges are quantum access structures if and only if they can be classified into 12 non-isomorphic types under hypergraph isomorphism, and these hypercyclic quantum access structures encompass all four hyperstars with three hyperedges. In prior work (Li et al., Inf. Sciences, vol. 664, 2024, 120202), efficient and perfect quantum secret sharing schemes were constructed for hyperstar access structures with three hyperedges using single photons in d -dimensional quantum systems. These schemes correspond to classical perfect secret sharing schemes with optimal information rates. However, for hypercyclic access structures with three hyperedges, the method described above fails to yield classical perfect secret sharing schemes with optimal information rates. In this work, we explicitly construct classical perfect secret sharing schemes with optimal information rates for these access structures by combining Simmons' geometric method with Shamir's threshold scheme. Subsequently, we employ single photons in d-dimensional quantum systems to build perfect QSS schemes upon these classical constructions. We introduce the concept of idealized information rate for minimal access structures in perfect QSS schemes. By extending the notion of efficiency proposed by Cabello [Phys. Rev. Lett., vol. 85, no. 26, p. 5635, 2000] for quantum key distribution protocols to QSS, we define the efficiency of minimally authorized subsets. Furthermore, we establish the relationship between the efficiency of minimally authorized subsets and the idealized information rate of minimal access structures. Finally, we rigorously prove that the QSS schemes constructed in this work achieve the highest efficiency among existing solutions.

Index Terms

Hypercycle, Quantuam access structure, Quantum secret sharing, Optimal information rate, Idealized information rate.

I. Introduction

With the continuous advancement of quantum technology, single particles and entangled states have emerged as crucial quantum resources for implementing quantum key distribution (QKD) protocols. For instance, in 1984, Bennett et al. [1] developed the world's first QKD protocol (BB84 protocol) using the polarization states of single photons, where two users share a secret key by exchanging single particles. In 1991, Ekert [2] proposed for the first time a QKD protocol based on the entanglement properties of Bell states. Subsequently, in 1992, Bennett et al. [3] introduced another QKD protocol (B92 protocol) utilizing non-orthogonal single-photon states. Since then, a series of QKD protocols based on single-particle states and entangled states have been proposed [4]–[7], and their security has been thoroughly analyzed [8]–[11]. However, most QKD protocols are designed for key distribution between two parties. In practical quantum networks, key distribution among multiple users is often required, making the extension of QKD protocols to multi-party scenarios a topic of significant interest. In 1995, Phoenix et al. [12] proposed the first multi-user QKD protocol based on single-particle states. Subsequently, various multi-user QKD protocols employing single particles, Bell states, GHZ states, and other resources have been introduced [13]–[17]. Quantum secret sharing (QSS) is a variant of QKD that enables secure secret distribution among multiple quantum-capable parties. The secret can be encoded in either classical states (as demonstrated in [18]) or quantum states (as presented in [19], [20]). The states distributed to participating parties are referred to as shares. Authorized subsets of participants (belonging to the access structure) can collaboratively reconstruct the secret, whereas unauthorized subsets abtain no information about it.

If the access structure of a QSS scheme consists of all subsets formed by at least t out of n participants, such a scheme is referred to as a (t, n)-threshold secret sharing scheme [21]–[28]. Hillery et al. [18] first proposed (2,2) and (3,3)-threshold schemes based on GHZ states. Subsequently, Wang and Cleve introduced (3,4)) [22] and $(t, 2t-1)$-threshold access structures [19] using local distinguishability of orthogonal multipartite entangled states and error-correcting codes, respectively. These works further extended to more general (t, n)-threshold access structures [23]–[28], enabling research on multiparty QKD protocols. However, the above-mentioned (t, n)-threshold access structures all correspond to special hypergraph access structure [29]. For example, considering a set of seven participants $P_1, P_2, ..., P_7$, let

$$\Gamma_0^{(1)} = \{ijkl \mid 1 \leq i < j < k < l \leq 7\},$$

here, the minimal authorized subsets $P_iP_jP_kP_l(1 =< i < j < k < l \leq 7)$ in $\Gamma_0^{(2)}$ are briefly denoted as $ijkl$. $\Gamma_0^{(1)}$ belongs to a threshold access structure, and it corresponds to a special hypergraph with the number of vertexs being 7, and each hyperedge contains different 4 vertexs.

This work was supported by the Youth Innovation Promotion Association, Chinese Academy of Sciences, under Grant 12201484.
Lei Li is with the School of Mechano-Electronic Engineering, Xidian University, Xi'an 710071, China (e-mail: lilei02@xidian.edu.cn).
Zhi Li is with the School of Mechano-Electronic Engineering, Xidian University, Xi'an 710071, China (e-mail: lizhi@xidian.edu.cn).

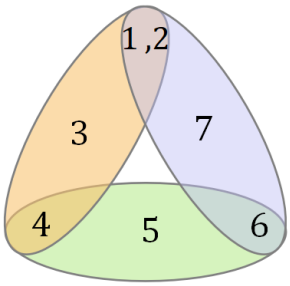

Fig. 1. The hypergraph corresponding to minimal access structure $\Gamma_0^{(2)}$.

However, significant theoretical progress has been made in developing multi-party QKD protocols based on special threshold access structures, most quantum network structures emerging from practical scenarios correspond to irregular hypergraphs [31]–[34]. For example, let $\Gamma_0^{(2)} = \{1234, 1267, 456\}$, then $\Gamma_0^{(2)}$ corresponds to a hypergraph which is an irregular one, see Fig.1. This requires the establishment of an efficient secret sharing protocol on the general access structure.

Any given hypergraph access structure can be realized using single-particle QSS schemes. However, not all hypergraph access structures can be implemented through multi-particle entangled-state QSS schemes, as the definition of quantum access structures is conditional [30]. Here, a quantum access structure specifically refers to a classical access structure that can be implemented by a multi-particle quantum secret sharing scheme. As proved in [30], a classical minimal access structure qualifies as a quantum minimal access structure if and only if any two of its authorized sets have non-empty intersection. For instance, as demonstrated in [19] that classical (t, n)-threshold access structures can serve as quantum threshold access structures if $n \leq 2t$. In this paper, we focus on constructing efficient QSS schemes for gengeral quantum access structures using single photons.

A. Related Work

As for the construction of an efficient secret sharing scheme based on general access structures, in the classical case, it is achieved by constructing a scheme with an optimal information rate [29], [35]–[38]. In addition, references [39]–[41] studied communication-efficient schemes in classical secret sharing for the reconstruction phase. But not as much in the quantum setting. References [26], [42], [43] showed that the quantum communication cost during secret recovery, however, these papers are also studied for special quantum access structures. Discussing from the number of edges contained in the hypergraph access structure, it can be known that the hypergraph access structure containing two hyperedges belongs to the ideal quantum access structure [29]. Reference [31] established an efficient quantum secret sharing scheme on the hyperstar quantum access structure containing three hyperedges by using single particles as information carriers.

B. Discussion

This paper conducts a study on hypercycle quantum access structure, establishes a classical secret sharing scheme with optimal information rates on it, and uses the parameters in these classical schemes to establish an efficient quantum secret sharing scheme on it by using single particles as information carriers. This scheme can provide a practical theoretical guarantee for the communication of light quantum network structure. Its practicality lies in the fact that this scheme is easy to implement under the existing experimental conditions, because the entire process does not require any quantum storage, and the data measured by participant can be saved.

In essence, these quantum access structures can also be used to establish secret sharing schemes using multi particle entangled states. However, at present, no systematic method has been given to establish an efficient quantum secret sharing scheme on them using multi particle entangled states. This problem can also be left as an open question. Although some scholars have also studied a large number of high-dimensional multi-particle entangled states and used the asymmetry exhibited by these high-dimensional multi-particle entangled states to improve the quantum communication efficiency of hierarchical key structures [32]–[34], however, no matter what, the starting point of these literatures is the preparation of high-dimensional entangled states and the design of efficient QKD schemes using these entangled states. How to design an efficient quantum secret sharing scheme for general quantum access structure using entangled states is a problem that needs further research.

C. Contributions

This paper conducts an in - depth study on the construction of efficient quantum secret sharing scheme on a hypercycle access structure containing three hyperedges. First, we theoretically investigate whether a hypercycle access structure is a quantum access structure, and we prove that a hypercycle access structure containing n hyperedges is a quantum access structure if and only if $n = 3$. These hypercycle quantum access structure are divided into 12 types in the sense of isomorphism. Furthermore,

we also prove that the hyperstar quantum access structure containing three hyperedges in [31] must be a hypercycle quantum access structure. Second, we construct an efficient quantum secret sharing scheme on these hypercycle quantum access structure containing three hyperedges. Since simply using the method in [31] cannot explicitly provide some classical secret sharing scheme with optimal information rates on some hypercycle access structure containing three hyperedges, we combine the idea of Simmons geometric construction [44] with the idea of Shamir threshold scheme and use the decomposition construction method [29] to complete the classical secret sharing scheme with optimal information rates for these access structures. Then, we use the parameters in these classical schemes to design a perfect quantum secret sharing protocol. In particular, we present all 83 hypercycle quantum access structure containing 7 participants, and calculate their optimal information rates using the above method. These results are given in Table 2 in the Appendix, which provide strong cases for designing lightweight efficient quantum secret sharing schemes. Third, inspired by the optimal information rate of the minimal access structure in the classical case, we propose the concept of idealized information rate for quantum minimal access structure. Meanwhile, by generalizing the concept of efficiency in the quantum key distribution protocol proposed in [45], we put forward the concept of efficiency of the minimal authorized subsets in the quantum secret sharing scheme, and then reveal the relationship between the efficiency of the minimal authorized subsets and the idealized information rate of the minimal quantum access structure. Furthermore, we prove that the perfect quantum secret sharing scheme established on the hypercycle quantum access structure with three hyperedges in this paper has the highest efficiency.

In this paper, a high-efficiency quantum secret sharing scheme is designed by combining single photons with the scheme with the optimal information rate in the classical scheme, which provides an idea for designing efficient schemes on general quantum access structures.

D. Organization

We give a brief review of CSS scheme and QSS scheme, and Simmons's geometry construction method in Section II. Then we construct perfect classical secret sharing schemes with optimal information rate for the hypercircle quantum access structures in Section III. In Section IV, we put forward the quantum secret sharing schemes on a hypercircle access structures with three hyperedges. In Section V, we propose the concept of the efficiency of the minimally authorized subset in the QSS scheme, and then the relationship between the efficiency of the minimally authorized subset and the idealized information rate of the minimally accessible structure is given, and we prove that the perfect quantum secret sharing scheme based on the hypercircle access structures with three hyperedges belongs to high efficient.

II. BACKGROUND

A. Notation

Let F_p be a finite field with p elements, where p is a prime. And let m be a positive integer with $p > m$, and F_p^m be the m-dimensional column vector space over F_p. We take the standard basis of C^p to be $|x\rangle$ where $|x| \in F_p$.

We use the notation $[m] := \{1, 2, ..., m\}$ and $[i, j] := \{i, i+1, ..., j\}$. For conciseness, denote the tuple $(A_1, A_2, ..., A_m)$ by $A_{[m]}$.

B. Hypergraph Access Structure

The relevant concepts in this subsection are mainly from Ref. [29].

Suppose that there are n participant set denoted as $P = \{P_1, P_2, ..., P_n\}$, and Γ is a collection composed of some subsets of P. If the participants included in the subsets of Γ can recover the key, then Γ is called the access structure on P, and the subsets of Γ are called authorized subsets. The access structure Γ has monotonicity: If $A \in \Gamma$ and $A \subseteq B$, then $B \in \Gamma$. The collection composed of the minimal authorized subsets (MAS) on the set P is called the minimal access structure on P, denoted as Γ_0. Obviously, $\Gamma_0 \subseteq \Gamma$. Each minimal access structure Γ_0 can be regarded as a hypergraph $H(P, \Gamma_0)$, where the participant set P represents the vertex set of the hypergraph $H(P, \Gamma_0)$, and each minimal authorized subset in Γ_0 can be regarded as a hyperedge in this hypergraph $H(P, \Gamma_0)$.

Ref. [29] denotes hypergraph as $H(V, E)$, where V is the vertex set and E represents the set consisting of all edges of the hypergraph. After the third section, we will use $H(P, \Gamma_0)$ instead of $H(V, E)$.

In this paper, all hypergraph refers to connected hypergraph.

Definition II.1. *Let $H(V, E)$ be a hypergraph. A set $R \subseteq V$ of nodes is a region of the hypergraph if there exists $I \subseteq E$ such that $R = (\cap_{E_i \in I} E_i) \setminus \big(\cup_{E_i \in (E \setminus I)} E_i\big)$. Furthermore, if $|I| = i$, then R is an i-region. For any $Z \subseteq V$, let $Rem(H, Z)$ be hypergraph $H' = (V', E')$, where $V' = V \setminus Z$ and $E' = \{E_i' = E_i \bigcap V' \neq \emptyset$, for any $E_i \in E\}$.*

It is important to note that, for any set Z, $Rem(H, Z)$ is no longer a substructure of H. Indeed some hypergraphs are a natural generalization of graphs like stars, paths, and cycles.

Definition II.2. *A hypergraph $H(V, E)$ is said to be a hyperstar with m hyperedges if the following condition hold:*
(1) $E = \{E_i | i \in [m]\}$;

(2) $\bigcap_{E_i \in E} E_i \neq \emptyset$*;*
(3)For any i*, there exists* $v \in V$ *such that* $v \in E_i$ *and* $v \notin E_j$*, for all* $j \neq i$*.*

Definition II.3. *[29] For a hypergraph* $H(V, E)$*, if there exists a hyperedge sequence* $(E_0, E_1, \cdots, E_{m-1})$ *in* E *such that*
(1) $E_i \cap E_{(i+1) \bmod m} \neq \emptyset, i = 0, 1, \cdots, m-1$*;*
(2) For any i*,* $E_i \cap E_j = \emptyset$*, where* $j \notin \{(i-1) \bmod m, i, (i+1) \bmod m\}$*,* $0 \leq i \leq m-1$*.*
Then this hypergraph is called a hypercycle with m *hyperedges.*

Definition II.4. *For a hypergraph* $H(V, E)$*, if there exists a hyperedge sequence* $(E_0, E_1, \cdots, E_{m-1})$ *in* E *such that*
(1)$E_i \cap E_{i+1} \neq \emptyset, i = 0, 1, \cdots, m-2$*;*
(2) For any i*,* $E_i \cap E_j = \emptyset$*, where* $i = 0, 1, \cdots, m-2$*,* $j \notin \{i-1, i, i+1\}$*.*
Then this hyperedge is called a hyperpath with m *hyperedges.*

C. Perfect Secret Sharing Scheme

Definition II.5. *[37] A scheme for sharing a secret key* K *in participant set* P *is called a perfect secret sharing scheme for realizing access structure* Γ *if it satisfies the following two conditions:*
(Recover) for an authorized subset $A \in \Gamma$ *of participants, if their shares are pooled together, the value of the secret key* K *can be determined.*
(Secret) for an unauthorized subset $B \neq \Gamma$ *of participants, even if all their shares are collected, no information about the value of* K *can be determined.*

Definition II.6. *[43] A quantum secret sharing scheme for an access structure* Γ *is the encoding and distribution of the secret in an arbitrary quantum state among* n *participants such that*
(Recoverability) any authorized set $A \in \Gamma$ *can recover the secret i.e. there exists some recovery operation which can decode the secret from the shares in* A*.*
(Secrecy) any unauthorized set $B \neq \Gamma$ *has no information about the secret.*

D. Mutually Unbiased Basis

Two sets of standard orthogonal bases $A_1 = \{|\phi_1\rangle, |\phi_2\rangle, \cdots, |\phi_p\rangle\}$, $A_2 = \{|\psi_1\rangle, |\psi_2\rangle, \cdots, |\psi_p\rangle\}$ in a p-dimensional Hilbert space are said to be mutually unbiased if they satisfy the relation $|\langle\phi_i|\psi_i\rangle| = \frac{1}{\sqrt{p}}$. A set B is said to be a mutually unbiased set of bases if any two sets of bases in the standard orthogonal bases set $B = \{A_1, A_2, \cdots, A_m\}$ in the p-dimensional Hilbert space are mutually unbiased. It follows from the literature [28] that when p is an odd prime, there are at most $p+1$ sets of mutually unbiased bases that can be found in the system. In particular, the computational basis is noted as $\{|k\rangle | k \in F_p\}$ and the remaining p groups of mutually unbiased bases are generally denoted as

$$\left|e_l^{(j)}\right\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \omega^{k(l+jk)} \left|k\right\rangle.$$

where $\omega = e^{\frac{2\pi i}{p}}$, j denotes the jth set of mutually unbiased bases and l denotes the lth vector in a given basis. These unbiased bases satisfy

$$\left|\left\langle e_l^{(j)} \middle| e_l^{(j')} \right\rangle\right| = \frac{1}{\sqrt{p}}, j \neq j'.$$

Let unitary transformation $U_{x,y} = X^x Y^y$, and act them on $|e_l^{(j)}\rangle$, then we get

$$\begin{aligned}
&U_{x,y} \left|e_l^{(j)}\right\rangle \\
&= X^x Y^y \left|e_l^{(j)}\right\rangle \\
&= X^x \left(\frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} \omega^{yn^2} |n\rangle\langle n|\right) \left(\sum_{k=0}^{p-1} \omega^{k(l+jk)} |k\rangle\right) \\
&= \frac{1}{\sqrt{p}} \left(\sum_{n=0}^{p-1} \omega^{xn} |n\rangle\langle n|\right) \left(\sum_{n=0}^{p-1} \omega^{yn^2} |n\rangle\langle n|\right) \left(\sum_{k=0}^{p-1} \omega^{k(l+jk)} |k\rangle\right) \\
&= \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \omega^{k(x+l+(j+y)k)} |k\rangle = \left|e_{(l+x)}^{(j+y)}\right\rangle.
\end{aligned}$$

where

$$X = \sum_{n=0}^{p-1} \omega^n \left|n\right\rangle\left\langle n\right|;$$

$$Y = \sum_{n=0}^{p-1} \omega^{n^2} \left|n\right\rangle\left\langle n\right|.$$

Definition II.7. *Assume that there is a well-established secret sharing scheme that implements a minimal access structure Γ_0. The information rate of this scheme is defined as*

$$\rho = \frac{H(K)}{\max_{P_i \in P}\{H(P_i)\}}$$

where K denotes the main key set, and $H(K)$ denotes the Shannon's entropy of the probability distribution of the set of shares $(p_s)_{s\in K}$, i.e., $H(K) = -\sum_{s\in K} p_s \log p_s$.

When the key space and share space are assigned with equal probability, the information rate of the scheme is $\rho = lb|K| / \max_{P_i \in P}\{lb|S(P_i)|\}$. Here $S(P_i)$ denotes the set where all possible shares of participant P_i are located, $H(P_i)$ denotes the entropy of the probability distribution of the set of shares $S(P_i)$, where $P_i \in P, i = 1, 2, \cdots, n$.

For a given access structure, the upper bound of the information rate in all achievable secret sharing schemes is called the optimal information rate, which was denoted as $\rho^*(\Gamma_0)$. It can be shown that the optimal information rate of perfect secret sharing schemes that implement an access structure does not exceed 1. An access structure with an optimal information rate of 1 is called an ideal access structure.

Lemma II.1. *Assume that Γ is an access structure with minimal access structure Γ_0 [47]. $l \geq 1$ is an integer. Let K be a specified key set and let $D_h = \{\Gamma_{h,1}, \Gamma_{h,2}, \cdot, \Gamma_{h,n_h}\}$ be an ideal decomposition of Γ_0 for the key set K, where $1 \leq h \leq l$. Let $P_{h,j}$ be the set of participants of the access structure $\Gamma_{h,j}$. For each participant P_i, define*

$$R = \sum_{i=1}^{l} |\{j : P_i \in P_{h,j}\}|$$

Then there exists a perfect secret sharing scheme that implements Γ with an information rate of $\rho = \frac{l}{R}$, where $R = Max\{R_i : 1 \leq i \leq n\}$.

Lemma II.2. *Let H be a hypercycles containing 3 hyperedges, and let B_1, B_2, B_3 be its 2-regions. Then for any $P_i \in B_r, P_j \in B_s$, $H(P_i) + H(P_j) \geq 3H(S)$, where $r, s = 1, 2, 3$ [29].*

E. Simmons 's Geometry Construction Method

The Simmons geometric construction [44] for secret sharing scheme can be thought of as a generalization of the Blakley threshold scheme [48]. The paper [49] improved Simmons' geometric construction [44], resulting in a modified scheme with higher information rate. we describe the scheme as follows [48].

The vectors in F_p^m are called points; the cosets of F_p^m relative to any 1-dimensional vector subspace, lines; the cosets of F_p^m relative to any 2-dimensional vector subspace, planes; the cosets of F_p^m relative to any $m-1$ dimensional vector subspace, hyperplanes. More generally, the cosets of F_p^m relative to any r -dimensional vector subspace $(0 \leq r \leq m)$ are called r-flats. In particular, 0-flats are points, 1-flats are lines, 2-flats are planes, and $(m-1)$-flats are hyperplanes. An r -flats is said to be incident with an s -flats if the r -flats contains or is contained in the s -flats. Then the point set F_p^m with the r-flats $(0 \leq r \leq m)$ and the incidence relation among them defined above is called the m -dimensional affine space over F_p, and denoted by $AG(m, F_p)$.

Let $\alpha_1 = (\alpha_{11}, \alpha_{12}, \cdots, \alpha_{1m})$ and $\alpha_2 = (\alpha_{21}, \alpha_{22}, \cdots, \alpha_{2m})$ be two distinct points in $AG(m, F_p)$, the line l passing through α_1 and α_2 is the set of points in the cosets $< \alpha_1 - \alpha_2 > + \alpha_2$, where $< \alpha_1 - \alpha_2 >$ is the 1-dimensional vector subspace by the non-zero vector $\alpha_1 - \alpha_2$. Hence the line passing through α_1 and α_2 is the point set

$$\{\mu(a_{11} - a_{21}, a_{12} - a_{22}, \cdots, a_{1m} - a_{2m}) + (a_{21}, a_{22}, \cdots, a_{2m})\},$$

or

$$\{\mu_1(a_{11}, a_{12}, \cdots, a_{1m}) + \mu_2(a_{21}, a_{22}, \cdots, a_{2m}) \mid \mu_1 + \mu_2 = 1\}.$$

where $\mu \in [0, 1]$.

More generally, the r -flat containing $r+1$ points $\alpha_1, \alpha_2, \cdot, \alpha_{r+1}$, which do not contain in any $(r-1)$-flat , has the parametric representation

$$\{\mu_1\alpha_1 + \mu_2\alpha_2 + \cdots + \mu_{r+1}\alpha_{r+1} \mid \mu_1 + \mu_2 + \cdots + \mu_{r+1} = 1\} \tag{1}$$

For convenience, we'll write this r-flat in (1) as Span $(\alpha_1, \alpha_2, \cdots, \alpha_{r+1})$. Suppose that V_D is a fixed line in $AG(m, F_p)$ with $\kappa = V_D$. Let V_I be a hyperplane such that $|V_I \bigcap V_D| = 1$; the key will be the unique point $V_I \bigcap V_D$. Every participant P_i will be given a share consisting of a set $d(P_i)$ of R_i points in V_I, and the set $d(P_i)$ chosen in such a way that, for every set B, we have

$$\text{Span}\left\{\sum_{\{i:P_i \in B\}} d(P_i)\right\} \cap V_D = \emptyset \Leftrightarrow B \notin \Gamma.$$

In other words, if the participants in the authorization set receive enough information vectors from V_I such that these vectors intersect with those of V_D and just happen to get the key $V_I \bigcap V_D$.

Since both the shares described in [49] and secret key are on the publicly known line segment V_D, [44] simplifies the points in the m-dimensional affine space that serve as shares into parameters by extracting the ideas from [49]. The specific description is given below. Assume that all $K_{i,j}$ and K_0 are public, where $K_{ij} \in V_I$, and $K_0 \in V_I$. Also, let L_{ij} be a line that contains K_{ij} and is parallel to V_D, and ε be the direction vector of $L_{i,j}$ and V_D. Let

$$V_D = \{K_0 + \lambda\varepsilon \mid \lambda \in F_p\};$$
$$L_{i,j} = \{K_{i,j} + \lambda_{i,j}\varepsilon \mid \lambda \in F_p, i \in [n], j \in [R_i]\}.$$

Let A be a $1 \times n$ matrix over F_p that satisfies $A \cdot \varepsilon = 1$, and let Π be the solution space of $AX = k$, where $k \in F_p$ is the secret key (when different values are taken, the corresponding Π is also different). After the straight lines V_D and L_{ij} intersect the plane Π respectively, we can obtain

$$K = K_0 + \lambda\varepsilon, \tag{2}$$

$$L_{i,j} \cap \Pi = K_{i,j} + \lambda_{i,j}\varepsilon. \tag{3}$$

By left-multiplying both sides of (2) and (3) by matrix A respectively, we have

$$\lambda = k - AK_0, \tag{4}$$

$$\lambda_{i,j} = k - AK_{i,j}. \tag{5}$$

for all i, j.

Since there is a one-to-one correspondence between λ and the point on V_D, and a one-to-one correspondence between λ_{ij} and the point on L_{ij}, we can take λ_{ij} as the participant P_i's shares, and take the domain element λ as the secret in this scenario. In this way, we only use numbers (instead of m-dimensional vectors) as shares and secrets. The distribution rules after such modification are as follows:

$$f_\Pi(D) = k - AK_0, \tag{6}$$

$$f_\Pi(P_i) = \{k - AK_{i,j} | 1 \le j \le R_i\}, i \in [n]. \tag{7}$$

An authorized subset B can calculate this secret key λ as a function of λ_{ij} as follows:

First, since

$$K_0 \in span(\sum_{\{i:P_i \in B\}} \bigcup_{j=1}^{R_i} K_{i,j}),$$

we can represent K_0 as follows,

$$K_0 = \sum_{\{i:P_i \in B\}} \sum_{j=1}^{R_i} \mu_{i,j} K_{i,j},$$

where $\sum_{\{i:P_i \in B\}} \sum_{j=1}^{R_i} \mu_{i,j} = 1$.

To make it easier to understand the idea of this transformation, we will provide an explanation with examples below, see Fig.2.

Let $\Gamma_0^{(3)} = \{134, 12, 23\}$. We set $p = 11$, $m = 3$. Let V_I be a plane meeting V_D in a point $K_0 = (0, 0, 0)$. And let $\varepsilon = (0, 0, 1)$, V_I is the plane $z = 0$. $K_{1,1}, K_{2,1}, K_{2,2}, K_{3,1}$ and $K_{4,1}$ are the points in V_I, where $K_{1,1} = (-1, 0, 0)$, $K_{2,1} = (0, 1, 0)$, $K_{2,2} = (1, 1, 0)$, $K_{3,1} = (1, -1, 0)$, $K_{4,1} = (1, 1, 0)$. A plane $\mathit{\Pi}$ that meets V_D in a point has the equation $ax + by + z = k$, where k is the secret and a, b are random numbers. Alice distributes the shares to the four participants as follows:

$$P_1 \leftarrow (k + a),$$
$$P_2 \leftarrow (k - b, k - a - b),$$
$$P_3 \leftarrow (k - a + b),$$
$$P_4 \leftarrow (k - a - b).$$

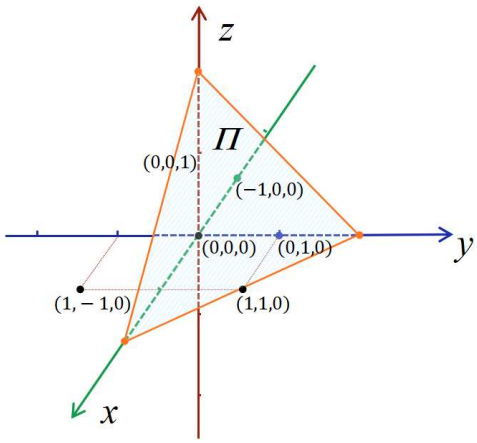

Fig. 2. Schematic diagram of the parameters of the secret share on the minimal access structure $\Gamma_0^{(3)}$, where Π stands for the blue plane.

In this way, we can obtain

$$\begin{aligned}\lambda &= k - AK_0 \\ &= k - A\sum_{\{i:P_i\in B\}}\sum_{j=1}^{R_i}\mu_{i,j}K_{i,j} \\ &= k - \sum_{\{i:P_i\in B\}}\sum_{j=1}^{R_i}\mu_{i,j}AK_{i,j} \\ &= k - \sum_{\{i:P_i\in B\}}\sum_{j=1}^{R_i}\mu_{i,j}\left(k-\lambda_{i,j}\right) \\ &= \sum_{\{i:P_i\in B\}}\sum_{j=1}^{R_i}\mu_{i,j}\lambda_{i,j}.\end{aligned}$$

Next we use Simmon's geometric construction method and decomposition construction method [47] to get the optimal information rate of the access structure $\Gamma_0^{(2)}$.

Example 1 Let $p = 11$, $m = 6$, $\Gamma_0^{(2)} = \{1234, 1267, 456\}$, seeing Fig.1. Let

$$\begin{aligned}V_I &= \{(x_1,x_2,x_3,x_4,x_5,x_6)|x_6 = 0\} \\ V_D &= \{(x_1,x_2,x_3,x_4,x_4,x_5,x_6)|x_i = 0, i\in[5]\} \\ \Pi &= \{(x_1,x_2,x_3,x_4,x_5,x_6)|A(x_1,x_2,x_3,x_4,x_5,x_6)^T = k\}\end{aligned}$$

where $A = (a,b,c,d,e,1)$ is a stochastic number and $a,b,c,d,e\in Z_{11}$, and Π intersects with V_D at k. Alice selects 9 points $K_{1,1}, K_{2,1}, K_{2,2}, K_{3,1}, K_{4,1}, K_{5,1}, K_{6,1}, K_{7,1}, K_{7,2}$ in V_I such that any three points among the following 10 points are not collinear,

$$K_{1,1}, K_{2,1}, K_{2,2}, K_{3,1}, K_{4,1}, K_{5,1}, K_{6,1}, K_{7,1}, K_{7,2}, K_0.$$

Here:

$$\begin{aligned}&K_{1,1} = (1,2,2,4,5,0)^T, K_{2,1} = (2,1,2,2,4,0)^T, \\ &K_{2,2} = (3,0,1,4,3,0)^T, K_{3,1} = (4,-1,0,1,1,0)^T, \\ &K_{4,1} = (5,5,-1,0,1,0)^T, K_{5,1} = (5,9,10,5,8,0)^T, \\ &K_{6,1} = (7,4,-3,7,-1,0)^T, K_{7,1} = (8,-5,-4,-3,0,0)^T \\ &K_{7,2} = (9,-6,-5,-4,-1,0)^T, K_0 = (0,0,0,0,0,0)^T.\end{aligned}$$

Alice publics $K_{1,1}$, $K_{2,1}$, $K_{2,2}$, $K_{3,1}$, $K_{4,1}$, $K_{5,1}$, $K_{6,1}$, $K_{7,1}$,$K_{7,2}$, K_0. Here

$$\begin{aligned}&V_D = \{K_0 + \lambda\varepsilon|\lambda\in F_{11}\}, \\ &L_{i,j} = \{K_{i,j} + \lambda_{i,j}\varepsilon|\lambda_{i,j}\in F_{11}\},\ \text{where } i\in[7], j\in[2].\end{aligned}$$

and $\varepsilon = (0, 0, 0, 0, 0, 1)$. Alice calculates

$$\lambda_{i,j} = k - AK_{i,j} (i \in [7], j \in [2]),$$

and pass $\lambda_{i,j}$ to P_i by secure channel, where

$$\begin{aligned}
\lambda_{1,1} &= k - AK_{1,1} = k - a - 2b - 2c - 4d - 5e,\\
\lambda_{2,1} &= k - AK_{2,1} = k - 2a - b - 2c - 2d - 4e,\\
\lambda_{2,2} &= k - AK_{2,2} = k - 3a - c - 4d - 3e,\\
\lambda_{3,1} &= k - AK_{3,1} = k - 4a + b - d - e,\\
\lambda_{4,1} &= k - AK_{4,1} = k - 5a - 5b + c - e,\\
\lambda_{5,1} &= k - AK_{5,1} = k - 6a + 3b - 5c + d - 5e,\\
\lambda_{6,1} &= k - AK_{6,1} = k - 7a - 4b + 3c - 7d + e,\\
\lambda_{7,1} &= k - AK_{7,1} = k - 8a + 5b + 4c + 3d,\\
\lambda_{7,2} &= k - AK_{7,2} = k - 9a + 6b + 5c + 4d + e.
\end{aligned}$$

For the minimal authorized subset 1234 in $\Gamma_0^{(2)}$, participant P_1, P_2, P_3, P_4 solve the following system of equations

$$\begin{aligned}
&\mu_{1,1}K_{1,1}+\mu_{2,1}K_{2,1}+\mu_{2,2}K_{2,2}+\mu_{3,1}K_{3,1}+\mu_{4,1}K_{4,1}=K_0,\\
&\mu_{1,1} + \mu_{2,1} + \mu_{2,2} + \mu_{3,1} + \mu_{4,1} = 1,
\end{aligned}$$

then obtain $(\mu_{1,1}, \mu_{2,1}, \mu_{2,2}, \mu_{3,1}, \mu_{4,1}) = (4, 8, 7, 6, 9)$.

For the minimal authorized subsets 1267 and 456, by solving the equations, and obtain respectively

$$\begin{aligned}
&(\mu_{1,1}, \mu_{2,1}, \mu_{2,2}, \mu_{6,1}, \mu_{7,1}, \mu_{7,2}) = (4, 4, 6, 1, 10, 9),\\
&(\mu_{4,1}, \mu_{5,1}, \mu_{6,1}) = (3, 1, 8).
\end{aligned}$$

For the minimal authorized subset 1234, participant P_1, P_2, P_3, P_4 can obtain secret key

$$\begin{aligned}
\lambda = &4(k - a - 2b - 2c - 4d - 5e)\\
&+ 8(k - 2a - b - 2c - 2d - 4e)\\
&+ 7(k - 3a - c - 4d - 3e)\\
&+ 6(k - 4a + b - d - e)\\
&+ 9(k - 5a - 5b + c - e)\\
&= k.
\end{aligned} \tag{8}$$

Similarly, the participant in the minimal authorized subsets 1347 and 2346 can both obtain the secret key k. It is easy to verify that the systems of equations in the above form established by any maximal non - authorized subsets in $\Gamma_0^{(2)}$ are all inconsistent. Therefore, they cannot obtain the secret key k.

III. HYPERCYCLE ACCESS STRUCTURE WITH THREE HYPEREDGES AND ITS OPTIMAL INFORMATION RATE

This section mainly studies the hypercycle access structure with three hyperedges and its optimal information rate. According to the definition of hypercycles, it is proved that all hyperstars with three hyperedges are hypercycles. Furthermore, all hypercycles with three hyperedges are classified in the sense of isomorphism. A total of 12 forms of hypercycle access structure with three hyperedges are presented, and the exact values of the optimal information rates for each type of access structure are calculated.

Since the minimal access structure Γ_0 corresponds to a hypergraph $H(P, \Gamma_0)$, for the sake of convenience, the hypergraph $H(P, \Gamma_0)$ corresponding to the minimal access structure Γ_0 is also denoted as Γ_0.

A. Types of hypercycle access structures with three hyper-edges

If Γ_0 is a connected hypergraph containing three hyperedges E_1, E_2, E_3, then there exists $E_i (i \in [3])$ such that $E_{(i-1) \bmod 3} \cap E_i \neq \emptyset$ and $E_i \cap E_{(i+1) \bmod 3} \neq \emptyset$.

Theorem III.1. *Let Γ_0 be a hypercycle containing $n (n \geq 3)$ hyperedges. Γ_0 is a quantum access structure if and only if $n = 3$. And there are 12 types of hypercycles in this case.*

Proof. **Necessity:** If Γ_0 is a quantum access structure, we will prove that $n > 3$ is impossible. Assume that $n > 3$, according to the definition of a hypercycle, for $i \in [n]$, then $E_i \cap E_{(i+1) \bmod 3} \neq \emptyset$, and for $j \notin \{(i-1) \bmod 3, i, (i+1) \bmod 3\}$, we

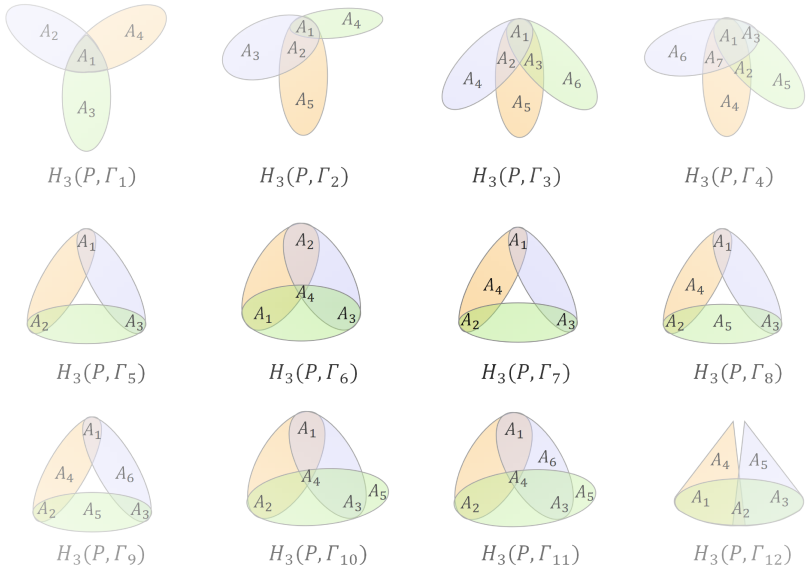

Fig. 3. Hypercycle quantum access structure containing 3 hyperedges, $H_3(P,\Gamma_i)(i\in[4])$ is a hyperstar.

have $E_i\cap E_j=\emptyset$. This indicates that the complement of the authorized subset E_i contains the authorized subset E_j, which contradicts the fact that Γ_0 is a quantum access structure.

Sufficiency: If Γ_0 is a hypercycle containing 3 hyperedges, then by the definition of a hypercycle, for $i\in[n]$, we have $E_i\cap E_{(i+1) \bmod 3}\neq\emptyset$. Therefore, according to the definition of a quantum access structure, Γ_0 is a quantum access structure.

If Γ_0 is a hypercycle quantum access structure, then there are a total of 12 types in the sense of isomorphism, and their algebraic representation is in the following form:

$$
\begin{aligned}
\Gamma_1 &= \{A_1A_2, A_1A_3, A_1A_4\},\\
\Gamma_2 &= \{A_1A_2A_4, A_1A_2A_5, A_1A_3\},\\
\Gamma_3 &= \{A_1A_2A_4, A_1A_2A_3A_5, A_1A_3A_6\},\\
\Gamma_4 &= \{A_1A_2A_4A_7, A_1A_2A_3A_5, A_1A_3A_6A_7\},\\
\Gamma_5 &= \{A_1A_2, A_1A_3, A_2A_3\},\\
\Gamma_6 &= \{A_1A_2A_4, A_1A_3A_4, A_2A_3A_4\},\\
\Gamma_7 &= \{A_1A_2A_4, A_1A_3, A_2A_3\},\\
\Gamma_8 &= \{A_1A_2A_4, A_1A_3, A_2A_3A_5\},\\
\Gamma_9 &= \{A_1A_2A_4, A_1A_3A_6, A_2A_3A_5\},\\
\Gamma_{10} &= \{A_1A_2A_4, A_1A_3A_4, A_2A_3A_4A_5\},\\
\Gamma_{11} &= \{A_1A_2A_4, A_1A_3A_4A_6, A_2A_3A_4A_5\},\\
\Gamma_{12} &= \{A_1A_2A_3, A_1A_2A_4, A_2A_3A_5\}.
\end{aligned}
$$

□

Theorem III.2. *Let Γ_0 be a hyperstar containing 3 hyperedges, then it must be a hypercycle.*

Proof. Without loss of generality, we assume that the access structure corresponding to Γ_0 is $\Gamma_0=\{A_1A_2, A_1A_3, A_1A_4\}$. Let $E_1=\{A_1A_2\}$, $E_2=\{A_1A_3\}$, $E_3=\{A_1A_4\}$, then there exists a hyperedge sequence (E_1,E_2,E_3) in this hyperstar such that for $i\in[3]$, $E_i\cap E_{(i+1) \bmod 3}\neq\emptyset$, and for $j\notin\{(i-1) \bmod 3, i, (i+1) \bmod 3\}$, $E_i\cap E_j=\emptyset$. According to Definition II.3, Γ_0 is a hypercycle. □

The hypergraph representations of the above 12 hypercycle quantum access structure are as follows, as shown in Fig.3.

B. The optimal information rate of hypercycle structures with 3 hyperedges

According to Theorems III.1 and III.2, the hyperstar quantum access structure containing 3 hyperedges must be a hypercycle quantum access structure. Reference [31] has given the explicit construction of the secret sharing scheme on these hyperstar access structures. So this subsection constructs a secret sharing scheme with optimal information rates, and gives these explicit construction on the hypercycle access structures $H_3(P, \Gamma_i)(i \in [5, 12])$ containing three hyperedges as shown in Fig.3.

For $P = \bigcup_{i=1}^{m} A_i$ are pairwise disjoint. where $m \in [4, 7]$. For convenience, let $A_i = \{P_1^{(i)}, P_2^{(i)}, \cdots, P_{m_i}^{(i)}, \}, i \in [m]$ below, where $P = \bigcup_{i=1}^{m} A_i$, and A_i and A_j are pairwise dispoint when $i \neq j$

Theorem III.3. *If the hypercycle containing 3 hyperedges is the quantum access structure Γ_i, then $\rho^*(\Gamma_i) = 1$, where $i \in [5, 6]$.*

Proof. First, an ideal secret sharing scheme is constructed to implement the access structure $\Gamma_5 = \{A_1A_2, A_1A_3, A_2A_3\}$.

The distributor Alice selects a secret key $s \in F_p$. When Alice wants to share the secret key among the participants, she gives each participant partial information, which is called shares. These shares are all secretly distributed. Each participant does not know the shares that Alice distributes to the other participants.

(I) Shares distribution phase

Alice applies the $(2, 3)$-threshold scheme to distribute a sub-shares to each subset A_1, A_2, A_3 respectively. The specific operations are as follows:

Alice selects 3 different non-zero elements in F_p, denoted as x_1, x_2, x_3 (here, it is required that $p > 4$), and uses them as the identities of participant in subsets A_1, A_2, A_3 respectively, where x_1, x_2, x_3 are public. Alice secretly selects an element a in F_p, sets $f(x) = s + ax$, and calculates $y_i = f(x_i), i \in [3]$. Further, Alice secretly selects $m_1 - 1$ elements in F_p, denoted as $y_1^{(1)}, y_2^{(1)}, \cdots, y_{m_1-1}^{(1)}$, and calculates $y_{m_1}^{(1)} = (y_1 - \sum_{i=1}^{m_1-1} y_i^{(1)}) \bmod p$. Then, Alice distributes the value of shares $y_i^{(1)}$ to $P_i^{(1)}, i \in [m_1]$.

Similarly, Alice distributes the value of shares $y_j^{(2)}$ to $P_j^{(2)}$, $j \in \{1, 2, \cdots, m_2\}$; distributes the value of shares $y_l^{(3)}$ to $P_l^{(3)}, l \in [m_3]$. By now, each participant in the participant set P has received their own shares.

(II) Reconstruct the subkey y_i. The participant of set A_1, A_2, A_3 respectively apply the (m_i, m_i)-threshold scheme share subkey y_1, y_2, y_3.

Accumulate the shares of all participant in A_1 to refactor the subkey y_1, i.e., $y_1 = \sum_{i=1}^{m_1} y_i^{(1)} \bmod p$. Similarly, accumulate the shares of all participant in A_2 and A_3 respectively to refactor the subkeys y_2 and y_3.

(III) Reconstruct the secret s.

First, present that the participants in the minimal authorized subset A_1 and A_2 use y_1 and y_2 to recover the secret s. They obtain the following system of linear equations on F_p by calculating y_1, y_2,

$$\begin{cases} s + ax_1 = y_1 \\ s + ax_2 = y_2 \end{cases}. \tag{9}$$

Since x_1 and x_2 are distinct, this system of equations has a unique solution on F_p, thus they obtain the secret s.

The minimal authorized subset A_1A_3, A_2A_3 can also refactor the secret s in a similar way respectively. It is easy to prove that the unauthorized subset in Γ_5 cannot obtain any information about the secret s.

When the participant in the minimal authorized subset share the secret s, each participant $P_j^{(i)}$ only receives one shares $y_{j_i}^{(i)}, j_i \in [m_i], i \in [3]$, so $\rho^*(\Gamma_5) = 1$.

Next we will prove that there also exists an ideal secret sharing scheme for the scenario of $\Gamma_6 = \{A_1A_2A_4, A_1A_3A_4, A_2A_3A_4\}$ to implement it. To share the secret s among the participant set P, let $s = s_1 + s_2$. Apply the $(|A_4|, |A_4|)$-threshold scheme to the participant in A_4 to share s_1. For the new access structure $\Gamma' = \{A_1A_2, A_1A_3, A_2A_3\}$, share s_2 according to the above proof method on Γ_5. Since the threshold schemes are all ideal, and independent schemes are used among non - intersecting participant, the final scheme for implementing access structure Γ_6 is also ideal, i.e. $\rho^*(\Gamma_6) = 1$. □

Lemma III.1. *Let Γ_i be a hypercycle containing 3 hyperedges, then $\rho^*(\Gamma_i) \leq \frac{2}{3}$, $i \in [7, 11]$.*

Proof. Since $\Gamma_i(i \in [7, 11])$ has at least one hyperedge with its own independent point set, let B_r and B_s be two non - empty 2-regions of Γ_i. It is easy to know from Lemma II.2 that for any $P_i \in B_r$, $P_j \in B_s$, $H(P_i) + H(P_j) \geq 3H(S)$. And then $H(P_i) \geq \frac{3H(S)}{2}$, so $max_{P_i \in V} H(P_i) \geq \frac{3H(S)}{2}$, and thus $\rho^*(\Gamma_i) \leq \frac{H(S)}{max_{P_i \in V} H(P_i)} \leq \frac{2}{3}, i \in [7, 11]$. □

Theorem III.4. *Let Γ_i be a hypercycle containing 3 hyperedges, then $\rho^*(\Gamma_i) = \frac{2}{3}, i \in [7, 11]$.*

Proof. According to Lemma III.1, we have $\rho^*(\Gamma_i) \leq \frac{2}{3}(i \in [7, 11])$. Now, we only need to construct an explicit perfect secret sharing for the hypercycle $\Gamma_i(i \in [7, 11])$ containing three hyperedges, and the information rate of this scenario should reach $\frac{2}{3}$. First, establish a perfect secret scheme for Γ_9.

Consider the following two decomposition. Let

$$\begin{aligned} &D_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}, \text{where} \Gamma_{1,1} = \{A_1A_2A_4\}, \\ &\Gamma_{1,2} = \{A_1A_3A_6, A_2A_3A_5\}; \end{aligned} \tag{10}$$

$$D_2 = \{A_1A_2A_4, A_1A_3A_6, A_2A_3A_5\}. \tag{11}$$

Obviously, D_1 is an ideal decomposition. $\Gamma_{1,1}$ can be realized by the $(3,3)$-threshold, and $\Gamma_{1,2}$ is a hyperstar containing two hyperedges. For D_2, we will use Simmons' geometric method to give an implementation scheme as follow. □

Distribution of shares in D_1 and reconstruction of the secret s.

Alice selects 6 different non-zero elements in F_p, denoted as $x_{[6]}$, and uses them as the identities of participant in the subset $A_{[6]}$ respectively. Here, $x_{[6]}$ is public. Note that the identity of each participant in A_i is the same, and $s \in F_p$ is the secret that participant will share.

(1) For $\Gamma_{1,1}$, Alice applies the $(3,3)$-threshold scheme to give a sub-shares to the participant subset in A_1, A_2, A_4 respectively.

Alice secretly selects two elements a_1, b_1 in F_p, sets $f_1(x) = s + a_1x + b_1x^2$, and calculates $f_1(x)(i \in \{1,2,4\})$. Further, Alice secretly selects $m_i - 1$ elements in F_p, denoted as $y_{i,1}^{(1,1)}, y_{i,2}^{(1,1)}, \cdots, y_{i,m_i-1}^{(1,1)}$, and calculates $y_{i,m_i}^{(1,1)} = (f_1(x_i) - \sum_{j_i=1}^{m_i-1} y_{i,j_i}^{(1,1)}) \bmod p$. Then, Alice sends the share $y_{i,j_i}^{(1,1)}$ to $P_{j_i}^{(i)}$ through a secure channel, $i \in \{1,2,4\}$, $j_i \in [m_i]$.

At this point, each participant in the participant set P has received their own shares.

The participants in A_i apply (m_i, m_i)-threshold scheme share subkey $f_1(x_i)$ respectively. For example, the shares of all participants in A_1 are accumulated to refactor the subkey $f_1(x_1)$, i.e., $f_1(x_1) = \sum_{j_1=1}^{m_1} y_{1,j_1}^{(1,1)} \bmod p$. Similarly, the shares of all participants in A_2 and A_4 are accumulated respectively to refactor the subkey $f_1(x_2)$ and $f_1(x_4)$.

As representatives in the subset A_1, A_2, A_4, $P_1^{(1)}, P_1^{(2)}, P_1^{(4)}$ solve the following system of linear equations:

$$\begin{cases} s + a_1x_1 + b_1x_1^2 = f_1(x_1) \\ s + a_1x_2 + b_1x_2^2 = f_1(x_2) \\ s + a_1x_4 + b_1x_4^2 = f_1(x_4) \end{cases}. \tag{12}$$

Since x_1, x_2, x_4 are distinct, this system of equations has a unique solution over F_p, and thus thesecret s is obtained.

(2) For $\Gamma_{1,2}$, Alice let $s = s_1 + s_2, s_1, s_2 \in F_p$.

Alice secretly selects $m_3 - 1$ elements from F_p, denoted as $y_{3,1}^{(1,2)}, y_{3,2}^{(1,2)}, \cdots, y_{3,m_3-1}^{(1,2)}$, and calculates $y_{3,m_3}^{(1,2)} = (s_1 - \sum_{j_3=1}^{m_3-1} y_{3,j_3}^{(1,2)}) \bmod p$. Then, she sends the share $y_{3,j_3}^{(1,2)}$ to $P_{j_3}^{(3)}$ through a secure channel, here $j_3 \in [m_3]$.

In the new structure $Remove(\Gamma_{1,2}, A_3) = \{A_1A_6, A_2A_5\}$ share secret key s_2. Since A_1A_6 and A_2A_5 are disjoint. Alice sets $f_2(x) = s + a_2x$, and secretly selects $m_i - 1$ elements from F_p, denoted as $y_{i,1}^{(1,2)}y_{i,1}^{(1,2)}, \cdots, y_{i,m_i-1}^{(1,2)}$, and calculates $y_{i,m_i}^{(1,2)} = (f_2(x_i) - \sum_{j,=1}^{m_i-1} y_{i,j_i}^{(1,2)}) \bmod p, i \in \{1,6\}$. Then, she sends the share $y_{i,j_i}^{(1,2)}$ to $P_{j_3}^{(i)}$ through a secure channel, $j_i \in [m_i], i \in \{1,6\}$. Alice sets $f_3(x) = s + a_3x$, and secretly selects $m_i - 1$ elements from F_p, denoted as $y_{i,1}^{(1,2)}y_{i,1}^{(1,2)}, \cdots, y_{i,m_i-1}^{(1,2)}$, and calculates $y_{i,m_i}^{(1,2)} = (f_3(x_i) - \sum_{i,=1}^{m_i-1} y_{i,j_i}^{(1,2)}) \bmod p, i \in \{2,5\}$. Then, she sends the share $y_{i,j_i}^{(1,2)}$ to $P_{j_3}^{(i)}$ through a secure channel, here $j_i \in [m_i], i \in \{2,5\}$.

$P_1^{(i)}$ $i \in \{1,2,3,5,6\}$acts as the representative in the subset A_i, and they recover the main secret s, in the following way.

The participant in set A_3 leverage $(|A_3|, |A_3|)$-threshold scheme share the subsecret s_1, that is, they calculate and get $s_1 = \sum_{j_3=1}^{m_3} y_{3,j_3}^{(1,2)} \bmod p$.

$P_1^{(1)}, P_1^{(6)}$ as representatives in subset A_1, A_6 respectively, solve the following system of linear equations:

$$\begin{cases} s_2 + a_3x_2 = f_2(x_1) \\ s_2 + a_3x_5 = f_2(x_6) \end{cases} \tag{13}$$

Since x_1, x_6 are distinct, this system of equations has a unique solution over F_p, and thus the subsecret s_2 is obtained.

$P_1^{(2)}, P_1^{(5)}$, as representatives in subset A_2, A_5, solve the following system of equations:

$$\begin{cases} s_2 + a_3x_2 = f_3(x_2) \\ s_2 + a_3x_5 = f_3(x_5) \end{cases} \tag{14}$$

Since x_2, x_5 are distinct, this system of equations has a unique solution over F_p, and thus the secret s_2 is obtained.

Finally, the minimal authorized subset $A_1A_3A_6$ (or $A_2A_3A_5$) calculates the secret s by $s = s_1 + s_2$.

Distribution of share in D_2 and reconstruction of the secret k.

Given $\Gamma_{2,1} = \{A_1A_2A_4, A_1A_3A_6, A_2A_3A_5\}$, let $V_I = \{(x_1, x_2, x_3, x_4, x_5, x_6) \mid x_6 = 0\}$, $V_D = \{(x_1, x_2, x_3, x_4, x_4, x_5, x_6) | x_i = 0, i = 1,2,3,4,5\}$, $\Pi = \{(x_1, x_2, x_3, x_4, x_5, x_6) | A(x_1, x_2, x_3, x_4, x_5, x_6)^T = k\}$, where $A = (a, b, c, d, e, 1)$, $a, b, c, d, e \in F_{11}$.

Suppose Π intersects V_D at k. Alice selects 8 points $K_{1,1}$, $K_{2,1}$, $K_{3,1}$, $K_{3,2}$, $K_{4,1}$, $K_{4,2}$, K_{51}, $K_{6,1}$ on V_I such that any three of the following 9 points $K_{1,1}$, $K_{2,1}$, $K_{3,1}$, $K_{3,2}$, $K_{4,1}$, $K_{4,2}$, K_{51}, $K_{6,1}$, $K_{7,1}$, K_0 are non-collinear.

Here

$$\begin{aligned}
&K_{1,1} = (1, a_1, 3, 4, 5, 0), a_1 \neq 2,\\
&K_{2,1} = (2, 1, a_2, 3, a_4, 0), a_2 \neq 2, a_4 \neq 4,\\
&K_{3,1} = (3, 0, b_2, a_3, 3, 0), b_2 \neq 1, a_3 \neq 2,\\
&K_{3,2} = (4, -1, c_2, b_3, 2, 0), c_2 \neq 0, b_3 \neq 1,\\
&K_{4,1} = (5, -2, -1, c_3, b_4, 0), c_3 \neq 0, b_4 \neq 1,\\
&K_{4,2} = (6, -3, -2, d_3, c_4, 0), d_3 \neq -1, c_4 \neq 0,\\
&K_{5,1} = (7, b_1, -3, -2, -1, 0), b_1 \neq -4,\\
&K_{6,1} = (8, -5, -4, -3, d_4, 0), d_4 \neq -2,\\
&K_0 = (0, 0, 0, 0, 0, 0).
\end{aligned}$$

Alice makes $K_{1,1}, K_{2,1}, K_{3,1}, K_{3,2}, K_{4,1}, K_{4,2}, K_{5,1}, K_{6,1}$ and K_0 be public. Since

$$\begin{aligned}
&V_D = \{K_0 + \lambda e | \lambda \in F_p\},\\
&L_{i,j} = \{K_{i,j} + \lambda_{i,j} e | \lambda_{i,j} \in F_p\}, \quad i \in [6],
\end{aligned}$$

here $e = (0, 0, 0, 0, 0, 1)$. Alice calculates $\lambda_{i,j} = k - AK_{i,j}, i \in [6], j \in [2]$, and share $\lambda_{i,j}$ among the participant in the set A_i through the (m_i, m_i)-threshold scheme.

Specifically, for $\lambda_{i,j}$, Alice secretly selects $m_i - 1$ elements in F_p, denoted as $y_{i,1,j}^{(2,1)} y_{i,2,j}^{(2,1)}, \cdots, y_{i,m_i-1,j}^{(2,1)}$, and calculates $y_{i,m_{i,j}}^{(2,1)} = (\lambda_{i,j} - \sum_{k_i=1}^{m_i-1} y_{i,k_{i,j}}^{(2,1)}) \bmod p$. Then, she sends the share $y_{i,j,k_i}^{(2,1)}$ to the $P_{k_i}^{(i)}$ through the secure channel, where $k_i \in [m_i], i \in [6]$. The participant in the set A_i calculates:

$$\lambda_{i,j} = \sum_{k_i=1}^{m_i} y_{i,k_i,j}^{(2,1)}) \bmod p. \tag{15}$$

$P_1^{(1)}, P_1^{(2)}, P_1^{(4)}$, as representatives in the subsets A_1, A_2, A_4, solve the following system of equations

$$\begin{cases}
\mu_{1,1} K_{1,1} + \mu_{2,1} K_{2,1} + \mu_{4,1} K_{4,1} + \mu_{4,2} K_{4,2} = K_0\\
\mu_{1,1} + \mu_{2,1} + \mu_{4,1} + \mu_{4,2} = 1
\end{cases} \tag{16}$$

then obtain $(\mu_{1,1}, \mu_{2,1}, \mu_{4,1}, \mu_{4,2})$.

By further substitution, they can obtain $\lambda = \mu_{1,1}\lambda_{1,1} + \mu_{2,1}\lambda_{2,1} + \mu_{4,1}\lambda_{4,1} + \mu_{4,2}\lambda_{4,2} = k$.

Similarly, for the minimal authorized subsets $A_1A_3A_6$ and $A_2A_3A_5$, k can be solved using the above method.

Since this scheme imposes restrictions on the selection of $K_{i,j}$, it ensures that the unauthorized subset in the access structure cannot obtain any information about the secret k. Therefore, this scheme is a perfect secret sharing scheme.

Furthermore, in this scheme, the shared secret key is (s, k), and the share received by the participant $P_1^{(i)} (i \in [6])$ is as follows:

$$\begin{aligned}
&P_1^{(1)} \text{ receives } (y_{1,1}^{(1,1)}, y_{1,1}^{(1,2)}, y_{1,1,1}^{(2,1)});\\
&P_1^{(2)} \text{ receives } (y_{2,1}^{(1,1)}, y_{2,1}^{(1,2)}, y_{2,1,1}^{(2,1)});\\
&P_1^{(3)} \text{ receives } (y_{3,1}^{(1,2)}, y_{3,1,1}^{(2,1)}, y_{3,1,2}^{(2,1)})\\
&P_1^{(4)} \text{ receives } (y_{4,1}^{(1,1)}, y_{4,1,1}^{(2,1)}, y_{4,1,2}^{(2,1)});\\
&P_1^{(5)} \text{ receives } (y_{5,1}^{(1,2)}, y_{5,1,1}^{(2,1)});\\
&P_1^{(6)} \text{ receives } (y_{6,1}^{(1,2)}, y_{6,1,1}^{(2,1)}).
\end{aligned} \tag{17}$$

Thus, the information rate of this scheme reaches $\frac{2}{3}$. Combining with the above analysis, we know that $\rho_c^* (H_3(P, \Gamma_9)) = \frac{2}{3}$.

By performing the following technical processing on the scheme of Γ_9, we can obtain a perfect secret sharing scheme on $\Gamma_i (i \in \{7, 8, 10, 11\})$ and the optimal information rate, as follows. Setting $A_6 = \emptyset$ in Γ_9, a similar scheme to Γ_9 can be applied to Γ_8, we can obtain $\rho^*(\Gamma_8) = \frac{2}{3}$. Similarly, by applying a scheme similar to that of Γ_8 to Γ_7, $\rho_C^*(\Gamma_7) = \frac{2}{3}$ can be obtained. Since $Rem(\Gamma_{10}, A_4) = \{A_1A_2, A_1A_3, A_2A_3A_5\} \cong \Gamma_7$, let $s = (s_1 + s_{2,1}, s_1 + s_{2,2})$, where s_1 is obtained from the participant in set A_4 through $(|A_4|, |A_4|)$-threshold scheme share. Perform two-layer decomposition on Γ_7 to construct share $(s_{2,1}, s_{2,2})$, finally we can get $\rho_C^*(\Gamma_{10}) = \frac{2}{3}$. Since $Rem(\Gamma_{11}, A_4) = \{A_1A_2, A_1A_3A_6, A_2A_3A_5\} \cong \Gamma_8$, using a similar method of finding the optimal information rate of Γ_{10}, we can get $\rho_C^*(\Gamma_{11}) = \frac{2}{3}$.

Theorem III.5. *If the hypergraph is a hypercycle Γ_{12} containing 3 hyperedges, then $\rho^*(\Gamma_{12}) = \frac{2}{3}$.*

Proof. Since $\Gamma_{12} = \{A_1A_2A_3, A_1A_2A_4, A_2A_3A_5\}$, and $Rem\{\Gamma_{12}, A_2\} = \{A_1A_3, A_1A_4, A_3A_5\}$ is a path, perform a 2-layer decomposition, and constructions on $Rem\{\Gamma_{12}, A_2\}$ are as follows:

$$D_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\},$$

where $\Gamma_{1,1} = \{A_1A_4\}$, $\Gamma_{1,2} = \{A_1A_3,\ A_3A_5\}$.

$$D_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\},$$

where $\Gamma_{2,1} = \{A_3A_5\}$, $\Gamma_{2,2} = \{A_1A_3,\ A_1A_4\}$.

Obviously, both D_1 and D_2 are two ideal coverages.

Let $s = (s_1 + s_{2,1}, s_1 + s_{2,2})$. The participant in set A_2 uses $(|A_2|, |A_2|)$-threshold scheme share s_1, D_1 can shares $s_{2,1}$, and D_2 shares $s_{2,2}$. As a simple calculation, $\rho^*(\Gamma_{12}) = \frac{2}{3}$ can be obtained.

Example III.1 Let ${\Gamma_0}^{(2)} = \{124, 136, 235\}$, and $D_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$,where$\Gamma_{1,1} = \{124\}, \Gamma_{1,2} = \{136, 235\}$, $D_2 = \{\Gamma_{2,1}\} = \{124, 136, 235\}$.

Obviously, D_1 is an ideal decomposition. $\Gamma_{1,1}$ can be realized by a $(3, 3)$-threshold. And $\Gamma_{1,2}$ is a hyperstar containing two hyperedges. The authorized sets in the two access structures can both recover the key s.

A solution for D_2 will be presented using Simmons' geometric method. Let

$$\begin{aligned}
&V_I = \{(x_1, x_2, x_3, x_4, x_5, x_6) | x_6 = 0\},\\
&V_D = \{(x_1, x_2, x_3, x_4, x_4, x_5, x_6) | x_i = 0, i \in [5]\},\\
&\Pi = \{(x_1, x_2, x_3, x_4, x_5, x_6) | A(x_1, x_2, x_3, x_4, x_5, x_6)^T = k\},
\end{aligned}$$

where $A = (a, b, c, d, e, 1)$, $a, b, c, d, e \in F_{11}$, and Π intersects V_D at k. Alice selects eight points $K_1, K_2, K_{3,1}, K_{3,2}$, $K_{4,1}$, $K_{4,2}$, $K_{5,1}$, $K_{6,1}$ such that any three of the following ten points $K_{1,1}, K_{2,1}, K_{3,1}, K_{3,2}, K_{4,1}$,$K_{4,2}, K_{5,1}, K_{6,1}, K_0$ are not collinear. Here,

$$\begin{aligned}
&K_{1,1} = (1, 2, 1, 4, 0, 0), K_{2,1} = (2, 1, 3, 2, 4, 0),\\
&K_{3,1} = (3, 0, 1, 1, 2, 0), K_{3,2} = (4, -1, 0, 2, 3, 0),\\
&K_{4,1} = (5, 1, -1, 0, 1, 0), K_{4,2} = (6, 1, -2, -1, 0, 0),\\
&K_{5,1} = (7, 1, -3, 3, -1, 0), K_{6,1} = (8, 4, -4, -3, 2, 0),\\
&K_0 = (0, 0, 0, 0, 0).
\end{aligned}$$

Alice makes $K_{1,1}, K_{2,1}, K_{3,1}, K_{3,2}, K_{4,1}, K_{4,2}, K_{5,1}, K_{6,1}, K_0$ be public. Since $V_D = \{K_0 + \lambda e\ |\lambda \in F_{11}\}$, $L_{i,j} = \{K_{i,j} + \lambda_{i,j}e | \lambda_{i,j} \in F_{11}\}, i \in [6]$.

Here $e = (0, 0, 0, 0, 0, 1)$. Alice calculates $\lambda_{i,j} = k - AK_{i,j} (i \in [6], j \in [2])$ as follows:

$$\begin{aligned}
&\lambda_{1,1} = k - AK_{1,1} = k - a - 2b - 1c - 4d,\\
&\lambda_{2,1} = k - AK_{2,1} = k - 2a - b - 3c - 2d - 4e,\\
&\lambda_{3,1} = k - AK_{3,1} = k - 3a - c - d - 2e,\\
&\lambda_{3,2} = k - AK_{3,2} = k - 4a + b - 2d - 3e,\\
&\lambda_{4,1} = k - AK_{4,1} = k - 5a - b + c - e,\\
&\lambda_{4,2} = k - AK_{4,2} = k - 6a + b + 2c + d,\\
&\lambda_{5,1} = k - AK_{5,1} = k - 7a - b + 3c - 3d + e,\\
&\lambda_{6,1} = k - AK_{6,1} = k - 8a - 4b + 4c + 3d - 2e.
\end{aligned}$$

For the minimal authorized subset 124 in ${\Gamma_0}^{(2)} = \{124, 136, 235\}$, participant P_1, P_2, P_4 solves the following system of equations

$$\begin{cases}
\mu_{1,1}K_{1,1} + \mu_{2,1}K_{2,1} + \mu_{4,1}K_{4,1} + \mu_{4,2}K_{4,2} = K_0\\
\mu_{1,1} + \mu_{2,1} + \mu_{4,1} + \mu_{4,2} = 1
\end{cases}$$

and gets $(\mu_{1,1}, \mu_{2,1}, \mu_{4,1}, \mu_{4,2}) = (-1, -6, 2, -5)$. Similarly, for the minimal authorized subsets 136 and 235, we can get

$$\begin{aligned}
&(\mu_{1,1}, \mu_{3,1}, \mu_{3,2}, \mu_{6,1}) = (2, 4, 10, 7),\\
&(\mu_{2,1}, \mu_{3,1}, \mu_{3,2}, \mu_{5,1}) = (7, -1, -8, 3).
\end{aligned}$$

For the minimal authorized subset 124, participant P_1, P_2, P_4 can get the secret $\lambda = -1(k - a - 2b - 1c - 4d) - 6(k - 2a - b - 3c - 2d - 4e) + 2(k - 5a - b + c - e) - 5(k - 6a + b + 2c + d) = k$.

For the minimal authorized subsets 136 and 235, secret k can be solved in the same way as above. □

In this example, according to Theorem III.4, a perfect secret - sharing scheme with a two - layer decomposition on hypercycle quantum access structure $\Gamma_0^{(2)}$ is presented. This scheme shares the secret (s,k). In the whole scheme, the share of each participant $P_i(i \in [6])$ can be obtained as follows:

$$\begin{aligned}
&P_1 \text{ receives } (y_{1,1}^{(1,1)}, y_{1,1}^{(1,2)}, y_{1,1,1}^{(2,1)});\\
&P_2 \text{ receives } (y_{2,1}^{(1,1)}, y_{2,1}^{(1,2)}, y_{2,1,1}^{(2,1)});\\
&P_3 \text{ receives } (y_{3,1}^{(1,2)}, y_{3,1,1}^{(2,1)}, y_{3,1,2}^{(2,1)})\\
&P_4 \text{ receives } (y_{4,1}^{(1,1)}, y_{4,1,1}^{(2,1)}, y_{4,1,2}^{(2,1)});\\
&P_5 \text{ receives } (y_{5,1}^{(1,2)}, y_{5,1,1}^{(2,1)});\\
&P_6 \text{ receives } (y_{6,1}^{(1,2)}, y_{6,1,1}^{(2,1)}),
\end{aligned} \tag{18}$$

where $y_{i,j}^{(2,1)} = \lambda_{i,j}$, so the optimal information rate of the access structure $\Gamma_0^{(2)}$ is $\frac{2}{3}$, i.e. $\rho_C^* \Gamma_0^{(2)} = \frac{2}{3}$.

IV. The QSS scheme based on the hypercycle access structure containing three hyperedges

In this section, we consider the establishment of the quantum secret sharing protocol on the minimal access structure Γ_9, where $\Gamma_9 = \{A_1A_2A_4, A_1A_3A_6, A_2A_3A_5\}$. According to the proof process of Theorem III.4, access structure Γ_9 are specifically shown in Fig.3.

A. System Definition

The model belongs to a mixture network structure that is made up of classical and quantum structures. In this model, $P = \bigcup_{i=1}^{6} A_i$, where each A_i is derived from the access structure Γ_9. We assume that each participant in P can make quantum states corresponding to the unbiased basis from the part D of the seciton I, operate these quantum states by unitary transform, and has the capability to measure the state of particles. Furthermore, we assume that the system key $K_j^{(0,i)}$ between Alice and each participant $P_j^{(i)}$, and the initial key $K^{(i,j)}$ between the sets A_i and A_j have been established using the BB84 protocol. We assumed that $K^{(i,j)}$ is owned by each participant from the sets A_i and A_j, and it is important to stress that $K_j^{(0,i)}$ and $K^{(i,j)}$ are absolutely secure as system keys.

Since this paper primarily focuses on the relationship between the information rate in classical secret sharing and the efficiency of quantum secret sharing built upon it, the model adopted here is a most fundamental one—assuming all participants are honest, with Eve being the only external attacker. We adopt the default setting where, during the share distribution phase, the sender transmits to each receiver an information quantum state sequence containing a total of n_I particles and a corresponding decoy-state sequence with n_E particles for detecting Eve's eavesdropping, here $n_E \ll p$, and $n_I \ll p$. Furthermore, the model assumes that the recipient has successfully received the sender's information accurately when the measurement results of all n_I quantum states are identical.

The Hash function is used in this paper as a polynomial hash [50]. Specifically, we make $PH = \{H_x : F_p^2 \to F_p, |x \in F_p\}$, where $H_x(y) = y_1 + y_2 x$, $y = (y_1, y_2) \in F_p^2$. It is well known that PH is almost universal in $\frac{2}{p}$.

B. Solution Description

In this subsection, let c be a primitive element of the finite field F_p. For convenience, let Alice's public identity be x_0, here $x_0 \in F_p$.

First, describe the process of using the quantum channel share the secret (s,k) for the minimal authorized subset $A_1A_2A_4$ in the access structure Γ_9 in Theorem III.4 of this paper. Since Γ_9 has two layers of decomposition $D_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$ and $D_2 = \{\Gamma_{2,1}\} = \{A_1A_2A_4, A_1A_3A_6, A_2A_3A_5\}$, where $\Gamma_{1,1} = \{A_1A_2A_4\}$, $\Gamma_{1,2} = \{A_1A_3A_6, A_2A_3A_5\}$. Therefore, for the minimal authorized subset $A_1A_2A_4$, we only need to consider the share of the secret (s,k) of the participant in these three sets A_1, A_2, A_4 in the minimal access structure $\Gamma_{1,1}$ and $\Gamma_{2,1}$.

Step 1. Distribution of shares

Alice manufactures the following particle sequence pairs according to the shares in the proof of Theorem III.4, as shown in Eq.(19-24). Each participant obtains the shares of the subset through measurement. Specifically, it is as follows.

(1) For the access structure $\Gamma_{1,1}$

(1.1) Alice first sends the information particle sequence (containing n_I particles) and the decoy particle sequence (containing n_E particles) (19-20) respectively for the participant $P_{j_i}^{(i)}$ in the set $A_i(i \in \{1,2,4\})$ according to the access structure $\Gamma_{1,1}$.

$$\left| e_{y_{i,j_i,1}^{(1,1)}}^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)} \right\rangle, \left| e_{y_{i,j_i,1}^{(1,1)}}^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)} \right\rangle, \cdots, \left| e_{y_{i,j_i,1}^{(1,1)}}^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)} \right\rangle, \tag{19}$$

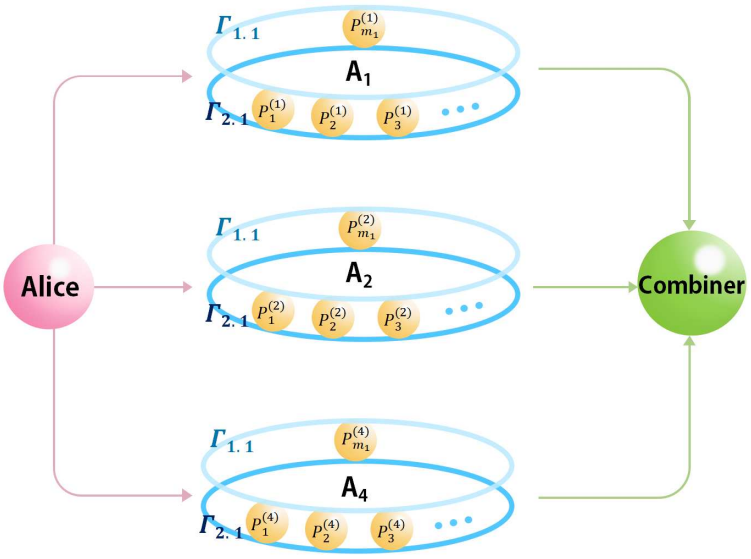

Fig. 4. Schematic diagram of the participant in the minimal authorized subset $A_1A_2A_4$ recovering the key (s,k)

$$\left|e_0^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)}\right\rangle,\left|e_0^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)}\right\rangle,\cdots,\left|e_0^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)}\right\rangle. \tag{20}$$

(1.2) After Alice confirms that participant $P_{j_i}^{(i)}$ has received the information particle sequence and decoy particle sequence, Alice announces the positions of these n_E decoy particles. $P_{j_i}^{(i)}$ uses the decoy particle sequence (20) received by the $H_{K_{j_i}^{(0,i)}}(x_0,x_i)$-th group of unbiased basis measurement and calculates the error rate of the measurement results. If the error rate is higher than the pre-set threshold, $P_{j_i}^{(i)}$ will stop this round and start a new one; otherwise, $P_{j_i}^{(i)}$ uses the Information Particle Sequence received by the $H_{K_{j_i}^{(0,i)}}(x_0,x_i)$-th group of unbiased basis measurement. If the measurement results are all equal, $P_{j_i}^{(i)}$ saves this result as their own share. Otherwise, $P_{j_i}^{(i)}$ requests Alice to start a new round again until the obtained measurement results are all equal.

(2) For the access structure $\Gamma_{2,1}$

(2.1) Alice sends the information particle sequence and decoy particle sequence (21-22) to the participant $P_{j_i}^{(i)}$ in the set A_4 respectively for the access structure $\Gamma_{2,1}$,

$$\left|e_{y_{i,j_i,1}^{(2,1)}}^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)}\right\rangle,\left|e_{y_{i,j_i,1}^{(2,1)}}^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)}\right\rangle,\cdots,\left|e_{y_{i,j_i,1}^{(2,1)}}^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)}\right\rangle, \tag{21}$$

$$\left|e_0^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)}\right\rangle,\left|e_0^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)}\right\rangle,\cdots,\left|e_0^{H_{K_{j_i}^{(0,i)}}(x_0,x_i)}\right\rangle, \tag{22}$$

where $j_4\in[m_4]$.

(2.2) Alice sends the information particle sequence and decoy particle sequence (23-24) to the participant $P_{j_i}^{(i)}$ in the set A_4 according to the access structure $\Gamma_{2,1}$.

$$\left|e_{y_{i,j_i,2}^{(2,1)}}^{H_{K_{j_i}^{(0,4)}}(x_0,x_4)}\right\rangle,\left|e_{y_{i,j_i,2}^{(2,1)}}^{H_{K_{j_i}^{(0,4)}}(x_0,x_4)}\right\rangle,\cdots,\left|e_{y_{i,j_i,2}^{(2,1)}}^{H_{K_{j_i}^{(0,4)}}(x_0,x_4)}\right\rangle, \tag{23}$$

$$\left|e_0^{H_{K_{j_4}^{(0,4)}}(x_0,x_4)}\right\rangle,\left|e_0^{H_{K_{j_4}^{(0,4)}}(x_0,x_4)}\right\rangle,\cdots,\left|e_0^{H_{K_{j_4}^{(0,4)}}(x_0,x_4)}\right\rangle, \tag{24}$$

where $j_4\in[m_4]$.

(2.3) participant $P_{j_i}^{(i)}$ performs steps similar to those in step (1.2) of this section to ensure obtaining the share sent by Alice to themselves, where $i\in\{1,2,4\}$, $j_i\in[m_i]$.

Step 2. Reconstruction of sub-keys

For ease of description, we assume that the participants in set A_i pass their respective shares in the protocol in the natural order.

Case (1): Present the reconstruction process of $f_1(x_i)$ for access structure $\Gamma_{1,1}$, where $i \in \{1,2,4\}$.

(1.1) $P_1^{(i)}$ chooses a random number $n_1^{(i)} \in F_p$, then creates the information particle sequence as shown in the following Eq.(25) and creates the decoy particle sequence as shown in Eq.(26), where $j_i = 1$.

$$\left|e^{n_1^{(i)}}_{log_c K(i,i)}\right\rangle, \left|e^{n_1^{(i)}}_{log_c K(i,i)}\right\rangle, \cdots, \left|e^{n_1^{(i)}}_{log_c K(i,i)}\right\rangle, \tag{25}$$

$$\left|e_0^{H_{K^{(i,i)}}(x_i,x_i)}\right\rangle, \left|e_0^{H_{K^{(i,i)}}(x_i,x_i)}\right\rangle, \cdots, \left|e_0^{H_{K^{(i,i)}}(x_i,x_i)}\right\rangle. \tag{26}$$

For convenience, denote the information particle sequence in Eq.(25) as $\left\langle \varphi_1^{(i)} \right|$. Then, $P_1^{(i)}$ randomly inserts the decoy particle sequence in Eq.(26) into the information particle sequence in Eq.(25) and sends the sequence composed of these information particles and decoy particles to $P_2^{(i)}$.

(1.2) After $P_2^{(i)}$ confirms the receipt of the sequence composed of these information particles and decoy particles, $P_1^{(i)}$ announces the positions of these n_E decoy particles. $P_2^{(i)}$ uses the decoy particle sequence received by the $H_{K^{(i,i)}}(x_i, x_i)$-th group of unbiased basis measurement and calculates the error rate of the measurement results. If the error rate is higher than the pre-set threshold, $P_2^{(i)}$ will stop this operation and require $P_1^{(i)}$ to start a new round; otherwise, he will continue with the following actions.

(1.3) $P_2^{(i)}$ removes these decoy particles and performs the unitary transformation $U_{y_{i,2}^{(1,1)},0}$ on the information particle sequence. The generated quantum state is denoted as $\left\langle \varphi_{n_i}^{(i)} \right|$. Then, $P_2^{(i)}$ creates n_E decoy particle state $\left|e_0^{H_{K^{(i,i)}}(x_i,x_i)}\right\rangle$ and randomly inserts them into the sequence composed of these n_I information quantum state $\left\langle \varphi_2^{(i)} \right|$. Then, $P_2^{(i)}$ sends the sequence composed of these information particles and decoy particles to $P_3^{(i)}$.

(1.4) The rest can be executed in the same way. Finally, $P_{n_i}^{(i)}$ will obtain n_I information quantum state and perform a unitary transformation $U_{y_{i,n_i}^{(1,1)},0}$. And denote the obtained quantum state as $\left\langle \varphi_{n_i}^{(i)} \right|$. Next, $P_{n_i}^{(i)}$ creates n_E decoy particle state $\left|e_0^{H_{K^{(i,i)}}(x_i,x_i)}\right\rangle$ and randomly inserts them into the sequence composed of these n_I information quantum state $\left\langle \varphi_{m_i}^{(i)} \right|$. Then, send the sequence composed of these information particles and decoy particles to $P_1^{(i)}$.

(1.5) $P_{n_i}^{(i)}$ announces the positions of these n_E decoy particles, uses the $H_{K^{(i,i)}}(x_i, x_i)$-th group of unbiased basis to measure the decoy particle sequence, and calculates the error rate of the measurement results. If the error rate is higher than the pre-set threshold, $P_1^{(i)}$ will stop this operation and require $P_{n_i}^{(i)}$ to start a new round; otherwise, he will continue with the following operations.

(1.6) $P_1^{(i)}$ removes these decoy particle and executes unitary transformation $U_{-log_c K(i,i)+y_{i,1}^{(1,1)},0}$ on the received information particle sequence. Then $P_1^{(i)}$ uses the n_I-th group of unbiased basis to measure the $n_1^{(i)}$ information quantum state. If the measurement results obtained are all equal, retain this measurement result; otherwise, return to step (1.1) to start a new round.

Case (2): The reconstruction of $\lambda_{i,j}$ for the access structure $\Gamma_{2,1}$, $i \in \{1,2,4\}$, $j \in [2]$.

(2.1) $P_1^{(i)}$ chooses a random number $n_1^{(i)} \in F_p$, then manufactures the information particle sequence as shown in the Eq.(25), and manufactures the decoy particle sequence of Eq.(30), where $j_i = 1$. For convenience, denote the information particle sequence in Eq.(26) as $\left\langle \varphi_1^{(i)} \right|$. Then, $P_1^{(i)}$ randomly inserts the decoy particle sequence in Eq.(26) into the information particle sequence in equation Eq.(25), and sends the sequence composed of these information particles and decoy particles to $P_2^{(i)}$.

(2.2) After $P_2^{(i)}$ confirms receiving these information particles and decoy particles, $P_1^{(i)}$ announces the positions of these n_E decoy particles. $P_2^{(i)}$ uses the $H_{K^{(i,i)}}(x_i, x_i)$-th group of unbiased basis to measure the decoy particle sequence received basis and calculates the error rate of the measurement results. If error rate is higher than the pre-set threshold, $P_2^{(i)}$ will stop this operation, and require $P_1^{(i)}$ to start a new round; otherwise, he will continue with the following operations.

(2.3) $P_2^{(i)}$ removes these decoy particles and performs the unitary transformation $U_{y_{i,2,j}^{(2,1)},0}$ on the information particle sequence. The resulting quantum state is denoted as $\left\langle \varphi_2^{(i)} \right|$. Then, $P_2^{(i)}$ manufactures n_E decoy particle state $\left|e_0^{H_{K^{(i,i)}}(x_i,x_i)}\right\rangle$ and randomly inserts them into the sequence composed of these n_I information quantum state $\left\langle \Psi_2^{(i)} \right|$. After that, $P_2^{(i)}$ sends the sequence composed of these information particles and decoy particles to $P_3^{(i)}$.

(2.4) The rest can be executed in the same way. Finally, $P_{n_i}^{(i)}$ performs the unitary transformation $U_{y_{i,2,j}^{(2,1)},0}$ on the n_I information quantum states, and the resulting quantum state is denoted as $\left\langle \Psi_{n_i}^{(i)} \right|$. Then $P_{n_i}^{(i)}$ creates n_E decoy particle state $\left|e_0^{H_{K^{(i,i)}}(x_i,x_i)}\right\rangle$ and randomly inserts them into the sequence composed of these n_I information quantum state $\left\langle \Psi_{n_i}^{(i)} \right|$. After that, $P_{n_i}^{(i)}$ sends the sequence composed of these information particles and decoy particles to $P_1^{(i)}$.

(2.5) $P_{n_i}^{(i)}$ announces the positions of these n_E decoy particles, uses the $H_{K^{(i,i)}}(x_i, x_i)$-th group of unbiased basis to measure the decoy particle sequence received, and calculates the error rate of the measurement results. If the error rate is higher than the pre-set threshold, $P_1^{(i)}$ will stop this operation and require $P_{n_i}^{(i)}$ to start a new round; otherwise, he will continue with the following operation.

(2.6) $P_1^{(i)}$ removes these decoy particles and performs the unitary transformation $U_{-log_c K(i,i)+y_{i,1,j}^{(2,1)},0}$ on the received information particle sequence. Then, $P_1^{(i)}$ uses the $n_1^{(i)}$-th group of unbiased basis to measure these n_I information quantum state, if they are all equal, then the measurement results are retained; otherwise, it will return to step (2.1) to start a new round.

Remark IV.1. *In Case (2), when $i \in [2]$, $P_1^{(i)}$ performs the unitary transformation $U_{y_{i,l,1}^{(2,1)},0}$; when $i = 4$, $P_1^{(4)}$ performs the unitary transformation $U_{y_{i,l,j}^{(2,1)},0}$, where $j \in [2]$.*

Step3. Recongstraction of the key.

When the combiner needs to access the minimally authorized subset $A_1A_2A_4$, Alice sets the public identity of the combiner to y_0 and the private key between the combiner and A_i to $C^{(0,i)}$, which is owed by each participant from the set A_i, where $(y_0, C^{(0,i)}) \in F_p^2$.

First, according to the system convention in the sub-key reconstruction of this section, if $P_1^{(i)}(i \in \{1,2,4\})$ uses the $n_1^{(i)}$-th group of unbiased basis to measure the n_I information quantum state obtained, and the measurement results are all equal, then $P_1^{(i)}$ has obtained the sub - key $f_1(x_i)$, or $\lambda_{i,j}$, where $i \in \{1,2,4\}, j \in [2]$.

Case (1): The reconstruction s for the access structure $\Gamma_{1,1}$.

(1.1) According to the operation diagram in Fig.4 of this scheme, for the access structure $\Gamma_{1,1}$, $P_1^{(i)}$ creates the following sequences

$$\left|e_{f_1(x_i)}^{log_c C^{(0,i)}}\right\rangle, \left|e_{f_1(x_i)}^{log_c C^{(0,i)}}\right\rangle, \cdots, \left|e_{f_1(x_i)}^{log_c C^{(0,i)}}\right\rangle, \tag{27}$$

$$\left|e_0^{H_{C^{(0,i)}}(y_0,x_i)}\right\rangle, \left|e_0^{H_{C^{(0,i)}}(y_0,x_i)}\right\rangle, \cdots, \left|e_0^{H_{C^{(0,i)}}(y_0,x_i)}\right\rangle. \tag{28}$$

Then, $P_1^{(i)}$ randomly inserts the decoy particle sequence in Eq.(28) into the information particle sequence in Eq.(27), and $P_1^{(i)}$ sends the sequence composed of these particles to combiners.

(1.2) After confirming the receipt of these information particles and decoy particles, $P_1^{(i)}(i \in \{1,2,4\})$ announces the positions of these n_E decoy particles. The combiner uses the $H_{C^{(0,i)}}(y_0, x_i)$-th group of unbiased basis to measure the decoy particle sequence received, and calculates the error rate of the measurement results. If the error rate is higher than the pre-set threshold, this operation will be stopped, and $P_1^{(i)}$ will be required to start a new round; otherwise, he will continue with the following operations.

(1.3) The ombiner removes these decoy particles, and then uses the $log_c c^{(0,i)}$-th group of unbiased basis to measure the n_I information quantum states. If all the obtained measurement results are equal, the measurement result is retained; otherwise, it will return to step (2.1) to start a new round.

(1.4) After obtaining $f_1(x_i)(i \in \{1,2,4\})$, the secret s is obtained by solving the system of equations (16).

Case (2): The reconstruction k for the access structure $\Gamma_{2,1}$.

(2.1) According to the operation diagram in Fig.4 of this scheme, for the access structure $\Gamma_{1,1}$, $P_1^{(i)}$ creates the following sequences

$$\left|e_{\lambda_{i,j}}^{log_c C^{(0,i)}}\right\rangle, \left|e_{\lambda_{i,j}}^{log_c C^{(0,i)}}\right\rangle, \cdots, \left|e_{\lambda_{i,j}}^{log_c C^{(0,i)}}\right\rangle, \tag{29}$$

$$\left|e_0^{H_{C^{(0,i)}}(y_0,x_i)}\right\rangle, \left|e_0^{H_{C^{(0,i)}}(y_0,x_i)}\right\rangle, \cdots, \left|e_0^{H_{C^{(0,i)}}(y_0,x_i)}\right\rangle. \tag{30}$$

Then, $P_1^{(i)}, (i \in \{1,2,4\})$ randomly inserts the decoy particle sequence in Eq.(30) into the information particle sequence in Eq.(29), and sends the sequence composed of these information particles and decoy particles to combiners.

(2.2) After confirming the receipt of the sequence composed of these information particles and decoy particles, $P_1^{(i)}(i \in \{1,2,4\})$ announces the positions of these n_e decoy particles. The combiner performs the $H_{C^{(0,i)}}(y_0, x_i)$-th group of unbiased basis measurement on the received decoy particle sequence and calculates the error rate of the measurement results. If error rate is higher than the pre-set threshold, this operation will be stopped, and $P_1^{(i)}(i \in \{1,2,4\})$ will be required to start a new round; otherwise, he will continue with the following operations.

(2.3) The combiners remove these decoy particle. Then, if the measurement results obtained from these n_I information quantum state using the $log_c c^{(0,i)}$ group of unbiased basis measurement are all equal, keep the measurement results; otherwise, return to step (2.2) and start a new round.

(2.4) After obtaining $\lambda_{i,j}(i \in \{1,2,4\}, j \in [2])$, solve the system of Eq.(16) to get the secret key k.

As can be seen from the above analysis, the minimal authorized set $A_1A_2A_4$ has recovered the secret (s, k) in this scheme. For the minimal authorized subsets $A_1A_3A_6$ and $A_2A_3A_5$ in Γ_9, the combiner can use a similar method as above to reconstruction the secret (s, k).

Remark IV.2. *Using the method of establishing QSS on Γ_9, QSS on minimal access structure $\Gamma_i(i \in \{7,8,10,11,12\})$ can also be similarly established.*

V. Idealized information rate and Efficiency

A. Idealized information rate

The information rate $\rho_c(\Gamma_0)$ is used to measure the efficiency of a perfect secret sharing scheme based on the minimal access structure Γ_0. A larger information rate value indicates a higher efficiency of the scheme. In this section, the concept of the information rate of a classical perfect secret sharing scheme is extended to a perfect QSS scheme, and the definition of the optimal idealized information rate of the minimal access structure is given. Here, the idealized information rate essentially ignores the interference of noise in the channel and does not consider the quantum state used for eavesdropping detection. The scheme in Section IV is used to calculate the optimal idealized information rate of the minimal access structure Γ. Below, we give the definition of the idealized information rate.

Definition V.1. *If there is a perfect QSS scheme that realizes minimal access structure Γ_0, and when the key space and share space are assigned with equal probability, then the idealized information rate of this scheme is defined as the ratio*

$$\rho_Q(\Gamma_0) = \frac{lb|S|}{\max_{P_i \in P}\{lb|Q(P_i)|\}}.$$

Here, $lb|Q(P_i)|$ represents the total number of particles of the space used by the distributed share set $S(P_i)$, and S represents the master key set, where $P_i \in P, i \in [n]$.

For a given access structure Γ_0, the upper bound of the idealized information rate of all perfect QSS scheme that realize it is called the optimal idealized information rate, denoted as $\rho_Q^*(\Gamma_0)$.

Remark V.1. *According to Definition V.1, to calculate $\rho_Q(\Gamma_0)$, we can first calculate the total number $lb|Q(P_i)$ used by the share set of each participant P_i.*

According to the scheme in Section IV, we first calculate the idealized information rate of each participant in this scheme, and then give the optimal idealized information rate of the access structure Γ_0. It is easy to see from the distribution phase of this scheme that the number of information particles received by each participant in the same set A_i is equal. Therefore, we only need to calculate the total number of particles of information received by the representative element $P_1^{(i)}$ in the set A_i, where $i \in [6]$. In this scheme, $lb|S| = lb_p p^2 = 2$, and the data of the information particles compiled by Alice in the distribution phase comes from the share of Alice in Theorem III.4. For example, in Theorem III.4, the share distributed by Alice to $P_1^{(1)}$ is $(y_{1,1}^{(1,1)}, y_{1,1}^{(1,2)}, y_{1,1,1}^{(2,1)}) \in F_p^3$. Thus, the total number of particles of information received by $P_1^{(1)}$ is $lb|Q(P_1^{(1)})| = lb_p p^{3\Gamma_I} = 3\Gamma_I$. In this way, the idealized information rate of $P_1^{(1)}$ is $\rho(P_1^{(1)}) = \frac{lb|S|}{lb|Q(P_1^{(1)})|} = \frac{2}{3}\frac{1}{\Gamma_I}$. Using a similar method, the total number of particles of information received by $P_1^{(i)}(i \in [2,6])$ and the idealized information rate can be obtained through calculation. See Table 1.

TABLE I
Total Number of information particle Received by participant in This Scheme and idealized information rate

	$P_1^{(1)}$	$P_1^{(2)}$	$P_1^{(3)}$	$P_1^{(4)}$	$P_1^{(5)}$	$P_1^{(6)}$
Total Number of information particle	$3\Gamma_I$	$3\Gamma_I$	$3\Gamma_I$	$3\Gamma_I$	$2\Gamma_I$	$2\Gamma_I$
Idealized Information Rate of Each participant	$2\frac{1}{\Gamma_I}$	$2\frac{1}{3\Gamma_I}$	$2\frac{1}{3\Gamma_I}$	$2\frac{1}{3\Gamma_I}$	$1\Gamma_I$	$1\Gamma_I$

According to the definition of idealized information rate, the idealized information rate of this scheme is $\frac{2}{3}\frac{1}{\Gamma_I}$. Furthermore, since this scheme is a perfect quantum secret sharing scheme based on the access structure Γ_0 with an optimal information rate of $\frac{2}{3}$, from Table 1 and the definition of the optimal idealized information rate, it can be known that the optimal idealized information rate of this scheme for the minimal access structure Γ_0 is also

$$\rho_Q^*(\Gamma_9) = \frac{2}{3}\frac{1}{\Gamma_I}.$$

Using the same method, it can be obtained that the optimal information rates of the minimal access structure $\Gamma_i)(i \in \{7,8,10,11,12\})$ are all $\frac{2}{3}\frac{1}{\Gamma_I}$.

B. Efficiency

In the QKD scheme, reference [45] gives the definition of efficiency in the scheme. This definition follows the approximation of the Holevo bound, requiring the optimization of quantum resources and the minimization of classical communication

overhead. If the scheme does not involve classical communication, the efficiency of the quantum key distribution scheme can be simplified to the following form:

$$\eta = \frac{c}{q},$$

where c represents the number of shared classical bits, and q represents the total number of particles prepared in the scheme, including the total information number of particles q_I and decoy particle q_E. In essence, from the perspective of the minimal authorized subsets contained in the access structure, the efficiency in reference [45] is studied for the case where the access structure contains only one authorized subset. Based on this, this paper derives the definition of efficiency from the minimal authorized subsets of the QSS scheme on the general access structure.

Definition V.2. *Let $\Gamma_0 = \{MAS_1, MAS_2, \cdots, MAS_l\}$ be a quantum access structure, where $MAS_i (i \in [l])$ is the minimal authorized subset, and Σ be a perfect quantum secret sharing scheme established on Γ_0. Then in scheme Σ, the efficiency of the minimal authorized subset MAS_i is defined as*

$$\eta(MAS_i) = \frac{c^{(i)}}{q_I^{(i)} + q_E^{(i)} + b_i^{(i)}},$$

where $c^{(i)}$ represents the number of shared classical bits of the minimal authorized subset MAS_i, $q_I^{(i)}$ represents the total number of all total number of particles required in the MAS_i scheme, and $q_E^{(i)}$ represents the total number of all total number of particles required for detecting Eve's eavesdropping in the scheme.

In this scheme, since the participant determines whether the information is accurate by checking whether the measurement results of Γ_I information particle are equal, there is no need for classical communication with the sender. On the other hand, in terms of preventing Eve's eavesdropping, the receiver can also determine whether there is interference from Eve by checking whether the measurement results of Γ_E eavesdropping particles are equal. This part also does not generate classical communication. Therefore, in this scheme, we can get $b^{(i)} = 0$.

The following presents the efficiency of three minimal authorized subsets.

$$\begin{aligned}
&\eta(A_1A_2A_4) \\
&= \frac{c_{A_1A_2A_4}}{q_{A_1A_2A_4}} \\
&= \frac{2}{(n_1 3\Gamma_I + 3n_2\Gamma_I + 3n_4\Gamma_I) + (3n_1\Gamma_E + 3n_2\Gamma_E + 3n_4\Gamma_E)} \\
&= \frac{2}{3}.\frac{1}{(\Gamma_I + \Gamma_E)(n_1 + n_2 + n_4)} \\
&= \frac{2}{3}\frac{1}{\Gamma_I}\frac{1}{(1+d)(n_1 + n_2 + n_4)} \\
&= \rho_Q^*(\Gamma_9)\frac{1}{(1+d)(n_1 + n_2 + n_4)}
\end{aligned} \tag{31}$$

Here, $d = \Gamma_E/\Gamma_I \circ$. Using the above calculation method, we can obtain:

$$\eta(A_1A_3A_6) == \rho_Q^*(\Gamma_9)\frac{1}{(1+d)(n_1 + n_3 + n_6)}, \tag{32}$$

$$\eta(A_2A_3A_5) == \rho_Q^*(\Gamma_9)\frac{1}{(1+d)(n_2 + n_3 + n_5)}. \tag{33}$$

From Eq.(31-33), it can be seen that if the idealized information rate of Γ_9 is higher, then the efficiency of each of its minimal authorized subsets is also higher. This also indicates that the idealized information rate can directly reflect the information - carrying efficiency of different participant in realizing the secret key.

From the above analysis, it can be known that this paper uses the parameters in the perfect classical secret sharing scheme and uses single photons to establish a perfect quantum secret sharing scheme on the minimal access structure Γ_9. Since the value of ρ_Q^* depends on the information rate of the perfect classical secret sharing scheme established on Γ_9, and these schemes all have the optimal information rate. This means that $\rho_Q^*(\Gamma_9)$ reaches the maximum in this scheme. Meanwhile, from Eq.(31-33), it can be known that the efficiency of the minimal authorized subsets in minimal access structure Γ_9 has all reached the optimal values.

Using the same method, the optimal idealized information rate on minimal access structure $\Gamma_i (i \in \{7, 8, 10, 11, 12\})$ and the optimal efficiency of their minimal authorized subsets can be obtained.

TABLE II
HYPER-CIRCLE ACCESS STRUCTURES WITH 7 PARTICIPANTS AND 3 HYPER-EDGES

Serial Number	Access Structure Γ	Serial Number	Access Structure Γ	Serial Number	Access Structure Γ
1	{12345,16,17}	29	{123456,123457,567}	57	{1234,1267,456}
2	{1234,156,17}	30	{123456,123457,234567}	58	{1234,167,456}
3	{123,145,167}	31	{123456,123457,4567}	59	{12345,23456,1267}
4	{12345,126,127}	32	{123456,12347,4567}	60	{12345,12367,3467}
5	{1234,1256,127}	33	{123456,12347,34567}	61	{12345,12367,23467}
6	{12345,1236,1237}	34	{123456,234567,12347}	62	{12345,1267,2367}
7	{12345,12346,12347}	35	{1234,4567,3567}	63	{1123456,12347,457}
8	{12345,12346,17}	36	{12345,23457,167}	64	{123456,12347,23457}
9	{126,12345,17}	37	{12345,1267,3457}	65	{123456,127,237}
10	{1234,156,157}	38	{12345,34567,127}	66	{123456,12347,3457}
11	{12345,1236,17}	39	{12345,167,567}	67	{1123456,1237,3457}
12	{1234,1235,167}	40	{12345,1267,567}	68	{123456,1237,347}
13	{1234,1256,17}	41	{12345,1267,3467}	69	{123456,1237,2347}
14	{1234,1235,1267}	42	{123456,12347,67}	70	{12345,1237,3467}
15	{1234,125,167}	43	{123456,17,67}	71	{12345,23467,1237}
16	{12345,12346,127}	44	{123456,3457,127}	72	{12345,23467,127}
17	{12345,1236,127}	45	{123456,127,67}	73	{12345,2367,127}
18	{1234,1235,1267}	46	{123456,3457,67}	74	{12345,1456,1267}
19	{12345,1236,147}	47	{123456,127,567}	75	{1234,1235,3467}
20	{1234,1256,137}	48	{1234,4567,127}	76	{1234,2567,125}
21	{12345,126,137}	49	{1234,1267,4567}	77	{12345,12346,457}
22	{12345,1236,1247}	50	{1234,4567,17}	78	{12345,12346,23457}
23	{1235,1367,1247}	51	{12345,1237,567}	79	{12345,126,267}
24	{12345,34567,1267}	52	{12345,567,17}	80	{12345,12346,3457}
25	{123456,123457,67}	53	{12345,34567,17}	81	{12345,1236,3457}
26	{123456,34567,127}	54	{12345,127,567}	82	{12345,1236,367}
27	{123456,1237,4567}	55	{12345,4567,127}	83	{12345,1236,2367}
28	{12345,12367,34567}	56	{12345,4567,17}		

APPENDIX

This section presents the hyper-circle access structure with 7 participants and 3 hyper-edges and their optimal information rates, as shown in Table II. The access structures corresponding to each serial number are distributed as follows: $\Gamma_1(1-7), \Gamma_2(8-18), \Gamma_3(19-22), \Gamma_4(23), \Gamma_5(24-27), \Gamma_6(28-34), \Gamma_7(35-47), \Gamma_8(48-56), \Gamma_9(57-58), \Gamma_{10}(59-69), \Gamma_{11}(70-74), \Gamma_{12}(75-83)$.

In Table II, the access structures numbered 1 - 23 belong to the hyper-star access structures, and the specific implementation schemes with optimal information rates have been given in [31]. According to Theorem III.3, the optimal information rate of the hyper-circle access structures numbered 24 - 34 is 1; according to Theorem III.4, the optimal information rate of the hyper-circle access structures numbered 35 - 74 is $\frac{2}{3}$; according to Theorem III.5, the optimal information rate of the hyper-circle access structures numbered 75 - 83 is $\frac{2}{3}$.

Using the methods in Section IV, efficient quantum secret sharing schemes for the above small-scale quantum access structures can be established. These schemes also provide a powerful tool for constructing quantum secret sharing schemes on quantum access structures formed by a larger number of participants.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China 12201484.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. 1, pp. 7–11, 2014. I
[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991. I
[3] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, 1992. I
[4] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, no. 14, pp. 3018–3021, 1998. I
[5] H. K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, 2012. I
[6] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 113, no. 14, p. 140501, 2014. I
[7] R. Jain, C. A. Miller, and Y. Shi, "Parallel device-independent quantum key distribution," *IEEE Trans. Inf. Theory*, vol. 66, no. 9, pp. 5567–5584, 2020. I
[8] H. K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999. I
[9] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000. I
[10] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, 2001. I
[11] V. Scarani et al., "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009. I
[12] S. J. D. Phoenix et al., "Multi-user quantum cryptography on optical networks," *J. Mod. Opt.*, vol. 42, no. 6, pp. 1155–1163, 1995. I
[13] Y. Guo, R. Shi, and G. Zeng, "Secure networking quantum key distribution schemes with Greenberger-Horne-Zeilinger states," *Phys. Scr.*, vol. 81, no. 4, p. 045006, 2010. I

[14] C. Y. Li, H. Y. Zhou, Y. Wang, and G. F. Deng, "Secure quantum key distribution network with bell states and local unitary operations," *Phys. Rev. Lett.*, vol. 22, no. 5, pp. 1049–1052, 2007. I
[15] P. Xue, C. F. Li, and G. C. Guo, "Conditional efficient multiuser quantum cryptography network," *Phys. Rev. A*, vol. 65, no. 2, p. 022317, 2002. I
[16] F. Gao, F. Z. Guo, Q. Y. Wen et al., "On the information-splitting essence of two types of quantum key distribution protocols," *Phys. Lett. A*, vol. 355, no. 3, pp. 172–175, 2005. I
[17] K. Chen and H. K. Lo, "Conference key agreement and quantum sharing of classical secrets with noisy GHZ states," in *Proc. Int. Symp. Inf. Theory*, Adelaide, Australia, 2005, pp. 1607–1611. I
[18] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, no. 3, pp. 1829–1834, 1999. I
[19] R. Cleve, D. Gottesman, and H. K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, no. 3, pp. 648–651, 1999. I, I
[20] D. Gottesman, "Theory of quantum secret sharing," *Phys. Rev. A*, vol. 61, no. 4, p. 042311, 2000. I
[21] H. Lu et al., "Secret sharing of a quantum state," *Phys. Rev. Lett.*, vol. 117, no. 3, p. 030501, 2016. I
[22] J. Wang et al., "Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states," *Phys. Rev. A*, vol. 95, no. 2, p. 022320, 2017. I
[23] T. Yuuki, O. Tatsuaki, and I. Nobuyuki, "Threshold quantum cryptography," *Phys. Rev. A*, vol. 71, no. 1, p. 012314, 2005. I
[24] A. Tavakoli, I. Herbauts, M. Zukowski, and M. Bourennane, "Secret sharing with a single d-level quantum system," *Phys. Rev. A*, vol. 92, no. 3, p. 030302, 2015. I
[25] V. Karimipour and M. Asoudeh, "Quantum secret sharing and random hopping: Using single states instead of entanglement," *Phys. Rev. A*, vol. 92, no. 3, p. 030301, 2015. I
[26] K. Senthoor and P. K. Sarvepalli, "Theory of communication efficient quantum secret sharing," in *IEEE Trans. Inf. Theory*, vol. 68, no. 5, pp. 3164–3186, May 2022, Errata for "Theory of Communication Efficient Quantum Secret Sharing", IEEE Trans. Inf. Theory, Volume: 70, Issue: 6, 4582–4584, 2024. I, I-A
[27] J. Wang et al., "Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states," *Phys. Rev. A*, vol. 95, no. 2, p. 022320, 2017. I
[28] H. Lai et al., "High-capacity (2,3) threshold quantum secret sharing based on asymmetric quantum lossy channels," *Quantum Inf. Process.*, vol. 19, p. 157, 2020. I, II-D
[29] G. Di Crecenzo and C. Galdi, "Hypergraph decomposition and secret sharing," *Discrete Appl. Math.*, vol. 157, no. 5, pp. 928–946, 2009. I, I-A, I-A, I-C, II-B, II-B, II.3, II.2
[30] A. Nascimento, J. Mueller-Quade, and H. Imai, "Improving quantum secret-sharing schemes," *Phys. Rev. A*, vol. 64, no. 4, p. 042311, 2001. I
[31] L. Li and Z. Li, "The quantum secret sharing schemes based on hyperstar access structures," *Inf. Sci.*, vol. 664, p. 120202, 2024. I, I-A, I-C, I-C, III-B, A
[32] M. Malik et al., "Multi-photon entanglement in high dimensions," *Nat. Photonics*, vol. 10, no. 4, pp. 248–252, 2016. I, I-B
[33] M. Pivoluska, M. Huber, and M. Malik, "Layered quantum key distribution," *Phys. Rev. A*, vol. 97, no. 3, p. 032312, 2018. I, I-B
[34] B. P. Lanyon et al., "Experimental violation of multipartite Bell inequalities with trapped ions," *Phys. Rev. Lett.*, vol. 112, no. 10, p. 100403, 2014. I, I-B
[35] M. H. Dehkordi and A. Safi, "The complexity of the connected graph access structure on seven participants," *J. Math. Cryptol.*, vol. 11, no. 1, pp. 25–35, 2017. I-A
[36] W. A. Jackson and K. M. Martin, "Perfect secret sharing schemes on five participants," *Des. Codes Cryptogr.*, vol. 9, no. 3, pp. 267–286, 1996. I-A
[37] M. V. Dijk, "On the information rate of perfect secret sharing schemes," *Des. Codes Cryptogr.*, vol. 6, no. 2, pp. 143–169, 1995. I-A, II.5
[38] M. Gharahi and M. H. Dehkordi, "The complexity of the graph access structures on six participants," *Des. Codes Cryptogr.*, vol. 67, no. 2, pp. 169–173, 2013. I-A
[39] W. Huang et al., "Communication efficient secret sharing," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7195–7206, 2016. I-A
[40] U. Martínez-Peñas, "Communication efficient and strongly secure secret sharing schemes based on algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 6, pp. 4191–4206, 2018. I-A
[41] R. Bitar and S. E. Rouayheb, "Staircase codes for secret sharing with optimal communication and read overheads," *IEEE Trans. Inf. Theory*, vol. 64, no. 2, pp. 933–943, 2018. I-A
[42] K. Senthoor and P. K. Sarvepalli, "Communication efficient quantum secret sharing," *Phys. Rev. A*, vol. 100, no. 5, p. 052313, 2019. I-A
[43] K. Senthoor and P. K. Sarvepalli, "Theory of communication efficient quantum secret sharing," *IEEE Trans. Inf. Theory*, vol. 68, no. 5, pp. 3164–3186, 2022. I-A, II.6
[44] G. J. Simmons, "How to really share a secret," *Lect. Notes Comput. Sci.*, vol. 403, pp. 390–448, 1990. I-C, II-E, II-E, II-E
[45] A. J. P. R. L. Cabello, "Quantum key distribution in the Holevo limit," *Phys. Rev. Lett.*, vol. 85, no. 26, pp. 5635–5638, 2000. I-C, V-B, V-B
[46] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Ann. Phys.*, vol. 191, no. 2, pp. 363–381, 1989.
[47] D. R. Stinson, "Decomposition constructions for secret sharing schemes," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 118–125, 1994. II.1, II-E
[48] G. Blakley, "Safeguarding cryptographic keys," in *Proc. Nat. Comput. Conf.*, Berlin, Germany, 1979, pp. 313–317. II-E, II-E
[49] D. R. Stinson, "An explication of secret sharing schemes," *Des. Codes Cryptogr.*, vol. 2, pp. 357–390, 1992. II-E, II-E, II-E
[50] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, 1979. IV-A