Communications in Theoretical Physics

Commun. Theor. Phys. **77** (2025) 025107 (11pp) https://doi.org/10.1088/1572-9494/ad8125

Masking quantum information in multipartite systems via Fourier and Hadamard matrices*

Chen-Ming Bai, Meng-Ya Wang, Su-Juan Zhang and Lu Liu**

Department of Mathematics and Physics, Shijiazhuang Tiedao University, Shijiazhuang 050043, China

E-mail: baichm@stdu.edu.cn

Received 2 July 2024, revised 27 September 2024
Accepted for publication 29 September 2024
Published 27 November 2024

Abstract

Quantum information masking (QIM) is a crucial technique for protecting quantum data from being accessed by local subsystems. In this paper, we introduce a novel method for achieving 1-uniform QIM in multipartite systems utilizing a Fourier matrix. We further extend this approach to construct an orthogonal array with the aid of a Hadamard matrix, which is a specific type of Fourier matrix. This allows us to explore the relationship between 2-uniform QIM and orthogonal arrays. Through this framework, we derive two distinct 2-uniform quantum states, enabling the 2-uniform masking of original information within multipartite systems. Furthermore, we prove that the maximum number of quantum bits required for achieving a 2-uniformly masked state is $2^n - 1$, and the minimum is $2^{n-1} + 3$. Moreover, our scheme effectively demonstrates the rich quantum correlations between multipartite systems and has potential application value in quantum secret sharing.

Keywords: multipartite systems, quantum information masking, Fourier matrix, orthogonal arrays

1. Introduction

In the realm of quantum mechanics, the no-cloning theorem stipulates that it is fundamentally impossible to produce an identical copy of an arbitrary unknown pure quantum state [1–3]. This seminal principle has catalyzed a cascade of related theorems that further articulate the nuanced nature of quantum information. Among these are the no-deleting theorem [4], the no-hiding theorem [5, 6], and the no-broadcasting theorem [7, 8], each contributing to our understanding of the distinctions between quantum and classical information paradigms. Concurrently, quantum entanglement has emerged as a cornerstone in the advancement of quantum information processing and quantum computation [9]. The phenomenon of quantum entanglement underpins several pivotal applications, including quantum key distribution [10], quantum teleportation [11, 12] and quantum secret sharing [13–16], highlighting the profound implications of quantum mechanics for secure communication and computational tasks.

Recently, the concept of quantum information masking has been introduced by Modi *et al* [17], who have also underscored a novel no-go theorem, termed the no masking theorem. This theorem asserts the impossibility of masking an arbitrary quantum state within bipartite quantum systems. Quantum information masking (QIM) has aroused widespread attention in the scientific community and many interesting and meaningful results on this topic have been obtained [18–33]. For instance, Li *et al* [18] studied how to mask quantum information in a multipartite scenario. In their masking protocol, it is also required that the original information is inaccessible to each local system. Furthermore, they have extended the definition of quantum information masking, as initially put forth by Modi *et al* [17], to encompass multipartite quantum systems. Wang *et al* [31] explored the possibility of partial masking of quantum information in multipartite systems using the generator matrices and stabilizer codes. Shen *et al* [32] gave the Latin-square construction of Abelian and Ising anyons in the Kitaev model and studied the maskable space configuration in anyonic space. In addition,

* This work was supported by the National Natural Science Foundation of China under Grant No. 12301590 and Natural Science Foundation of Hebei Province under Grant No. A2022210002.
** Author to whom any correspondence should be addressed.

Liu *et al* [23] devised a photonic QIM machine using time-correlated photons to experimentally investigate the properties of qubit masking and demonstrated the transfer of quantum information into bipartite correlations and its faithful retrieval. However, all of the above studies are limited to the case of 1-uniform quantum information masking. Afterward, Shi and Li *et al* [27] proposed the concept of k-uniform QIM in multipartite systems and indicated the relation between quantum error-correcting codes in heterogeneous systems and quantum information masking. The studies on the above-mentioned quantum information masking can facilitate the advancement of quantum secret sharing.

In 2013, Arnaud and Cerf [33] introduced the concept of k-uniform states, which has since become a pivotal framework in quantum information theory. Building upon this foundation, Goyeneche and Zyczkowski [34] demonstrated that orthogonal arrays, a mathematical structure with profound implications for quantum state characterization, can be derived from Hadamard matrices. In addition, they established a link between the orthogonal arrays and k-uniform states. In this work, we establish 1-uniform QIM within multipartite quantum systems by employing a Fourier matrix. Subsequently, we focus on a special case of the Fourier matrix, specifically when the dimension $d=2$. Under these conditions, the Fourier matrix is equivalent to a Hadamard matrix, which is a key component in our subsequent analysis. Capitalizing on the foundational work of Goyeneche *et al* [34] regarding the derivation of 2-uniform states, we proceed to manipulate these states further. By applying an X-gate to each qubit within the 2-uniform state. we successfully generate an alternative 2-uniform state. Utilizing these states, the original quantum information encoded in the form $\alpha|0\rangle+\beta|1\rangle$ can be effectively masked in a 2-uniform manner across multipartite systems. Our research further enriches 1-uniform QIM and 2-uniform QIM, and has significant application value for quantum secret sharing.

The paper is organized as follows. In section 2, we give some necessary definitions about the masking of quantum information and some related concepts. In section 3, we firstly implement a 1-uniform quantum information masking in high-dimensional multipartite systems using the Fourier matrix method. In addition, we propose a 2-uniform quantum information masking and offer a specific example for $n=4$. In section 4, we provide an application of QIM, which is the recovery stage of quantum secret sharing. In section 5, we draw a conclusion.

2. Preliminaries

In this section, we will mainly give some important definitions of quantum information masking [17, 18, 27] Fourier matrices and orthogonal arrays [34–37].

2.1. Quantum information masking

In [18], Li *et al* generalized the definition of quantum information masking to multipartite quantum systems.

Definition 1. [18] An operation M is said to mask quantum information contained in states $\{|a_k\rangle_{A_1}\in\mathcal{H}_{A_1}\}$ by mapping them to states $\{|\Psi_k\rangle\in\otimes_{j=1}^{n}\mathcal{H}_{A_j}\}$ such that all the marginal states $|\Psi_k\rangle$ are identical, i.e.,

$$\rho_{A_j}=\mathrm{Tr}_{\widehat{A_j}}(|\Psi_k\rangle\langle\Psi_k|),\quad j\in\{1,2,\cdots,n\},\tag{1}$$

have no information about the value of k, and $\widehat{A_j}$ denotes the set $\{A_1,A_2,\cdots,A_n\}\setminus\{A_j\}$.

To simplify writing, we use $\mathbb{C}$ to represent the complex number field and $\mathbb{C}^d$ to represent a d-dimensional Hilbert space. Therefore, the concept of QIM can be rewritten as follows.

Definition 2. An operation M is said to mask quantum information contained in states $|l\rangle\in\mathbb{C}^d$ by mapping them to quantum states $\{|\Psi_l\rangle\in(\mathbb{C}^d)^{\otimes n}\colon l=0,1,\cdots,d-1\}$ such that all the marginal states $|\Psi\rangle$ are identical, i.e.,

$$\rho_j=\mathrm{Tr}_{\hat{j}}(|\Psi\rangle\langle\Psi|),\quad j\in\{1,2,\cdots,n\},\tag{2}$$

where j denotes the set $\{1,2,\cdots,n\}\setminus\{j\}$.

For quantum information masking in multipartite systems, collusion between some subsystems would then reveal the encoded quantum information. Therefore, to avoid such collusion, Shi and Li *et al* [27] proposed the definition of k-uniform quantum information masking. The following will provide the specific definition of 2-uniform masking.

Definition 3. An operation M is said to mask quantum information contained in states $|l\rangle\in\mathbb{C}^2$ by mapping them to quantum states $\{|\Psi_l\rangle\in(\mathbb{C}^2)^{\otimes n}\colon l=0,1\}$ such that all the reductions to 2 parties of $|\Psi\rangle=\alpha|\Psi_0\rangle+\beta|\Psi_1\rangle$ are identical, i.e.,

$$\rho_{ij}=\mathrm{Tr}_{\hat{ij}}(|\Psi\rangle\langle\Psi|),\tag{3}$$

where $\hat{ij}$ denotes the set $\{1,2,\cdots,n\}\setminus\{i,j\}$ and $i,j\in\{1,2,\cdots,n\}$ $(i\neq j)$.

2.2. Fourier matrices and orthogonal arrays

In this section, we present the Fourier matrix and orthogonal arrays with the intention of developing a QIM scheme. Consequently, the Fourier matrix can be expressed in the following manner:

$$F_d=\begin{pmatrix}1&1&1&\cdots&1&1\\1&\omega&\omega^2&\cdots&\omega^{d-2}&\omega^{d-1}\\1&\omega^2&(\omega^2)^2&\cdots&(\omega^{d-2})^2&(\omega^{d-1})^2\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\1&\omega^{d-2}&(\omega^2)^{d-2}&\cdots&(\omega^{d-2})^{d-2}&(\omega^{d-1})^{d-2}\\1&\omega^{d-1}&(\omega^2)^{d-1}&\cdots&(\omega^{d-2})^{d-1}&(\omega^{d-1})^{d-1}\end{pmatrix},\tag{4}$$

where $\omega=\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}}$. The matrix F_d is a unitary matrix over the complex space $\mathbb{C}$, characterized by the property that each row (or each column) of F_d is orthogonal to every other row (or column).

Additionally, we employ techniques based on orthogonal arrays for masking quantum information. Moving forward, we will now present the definition of orthogonal arrays.

Definition 4. [35] Let A be a matrix of dimensions $r \times N$ whose elements are drawn from a set $S = \{s_1, s_2, \cdots, s_d\}$, if every $r \times k$ submatrix of A contains each k-element subset of S with equal frequency, then A is said to be an orthogonal array, denoted as OA(r, N, d, k).

For an N-particle multipartite pure state, if all of its k particle reduced states are maximally mixed, it is called a k-uniform state. Goyeneche and Zyczkowski [34] provided two important basic conditions for establishing k-uniform states through orthogonal arrays. We term this the fundamental property of orthogonal arrays, as illustrated below.

(1) Each subarray composed of any k columns from the orthogonal array contains all k-element arrays formed by the elements of the set S, and each k-element array has the same number of repetitions;
(2) A subarray consisting of any $N-k$ columns of an orthogonal array contains an $(N-k)$ tuple array in each row, and each $(N-k)$ tuple array is not repeated.

3. Quantum information masking in multipartite systems

In this section, we first use a Fourier matrix to achieve 1-uniform quantum information masking in multipartite systems. Then, we consider a special case to obtain 2-uniform quantum information masking.

3.1. 1-uniform quantum information masking

To construct maskable quantum states, we adopt the Fourier matrices F_d, where d is odd prime. Furthermore, we can construct a matrix $G = F_d \otimes F_d$ of order N, where $N = d^2$. Then we delete the first column elements of G and transform the remaining elements through a mapping $\varphi: \omega^i \mapsto i$. Therefore, we can get the new matrix G_N^0, and it is represented as

$$G_N^0 = (\vec{\alpha}_{0,1}, \vec{\alpha}_{0,2}, \cdots, \vec{\alpha}_{0,N})^{\mathrm{T}}, \tag{5}$$

where $\vec{\alpha}_{0,j}$ is an $(N-1)$-dimensional row vector, $j = 1, 2, \cdots, N$.

Furthermore, we define a permutation set $\{\pi_0, \pi_1, \cdots, \pi_{d-1}\}$, with each π_l represented as a mapping such that $i \mapsto (i+l) \bmod d$, where i, $l = 0, 1, \cdots, d-1$. Therefore, we transform all elements of G_N^0 according to the permutation $\pi_l \in \{\pi_0, \pi_1, \cdots, \pi_{d-1}\}$ to obtain the matrix

$$G_N^l = (\vec{\alpha}_{l,1}, \vec{\alpha}_{l,2}, \cdots, \vec{\alpha}_{l,N})^{\mathrm{T}}. \tag{6}$$

According to the row vector $|\vec{\alpha}_{l,j}\rangle$ in the matrix G_N^l, we construct the quantum state

$$|\Psi_l\rangle = \frac{1}{\sqrt{d^2}} \sum_{j=1}^{N} |\vec{\alpha}_{l,j}\rangle. \tag{7}$$

Due to the unitarity of the Fourier matrix, it can be obtained that

$$\langle \vec{\alpha}_{l,j} | \vec{\alpha}_{l,k} \rangle = 0, \tag{8}$$

where $j \neq k$ and j, $k \in \{1, 2, \cdots, N\}$.

Let $|0\rangle$, $|1\rangle$, $\cdots$, $|d-1\rangle$ be an orthogonal normalized basis of $\mathbb{C}^d$, and define the following physical process:

$$|l\rangle \mapsto |\Psi_l\rangle = \frac{1}{\sqrt{d^2}} \sum_{j=1}^{N} |\vec{\alpha}_{l,j}\rangle. \tag{9}$$

Since G_N^l is obtained by applying different permutations π_l to G_N^0, each row of G_N^l does not have corresponding equal elements, and due to the orthogonality of F_d, we can derive

$$\langle \vec{\alpha}_{l,i} | \vec{\alpha}_{m,i} \rangle = 0, \quad \langle \vec{\alpha}_{l,i} | \vec{\alpha}_{m,j} \rangle = 0, \tag{10}$$

where l, $m \in \{0, 1, \cdots, d-1\}$ and i, $j \in \{1, 2, \cdots, N\}$.

Theorem 1. *Let* $\mathrm{F_d}$ *be a Fourier matrix of odd prime order, then the quantum state* $|\vec{\alpha}\rangle = \sum_{l=0}^{d-1} \alpha_l |l\rangle$ *can be masked into* $|\Psi_{\vec{\alpha}}\rangle = \sum_{l=0}^{d-1} \alpha_l |\Psi_l\rangle$ *thought the process defined in equation (9), where* $\sum_{l=0}^{d-1} \alpha_l = 1$.

Proof. Though equation (9), we can deduce that

$$|\Psi_{\vec{\alpha}}\rangle = \frac{1}{\sqrt{d^2}} \sum_{l=0}^{d-1} \sum_{j=1}^{N} \alpha_l |\vec{a}_{l,j}\rangle. \tag{11}$$

Therefore, we can easily calculate the partial trace of $|\Psi_{\vec{\alpha}}\rangle \langle \Psi_{\vec{\alpha}}|$, i.e.,

$$\rho_i = \mathrm{Tr}_{\hat{i}} [|\Psi_{\vec{\alpha}}\rangle \langle \Psi_{\vec{\alpha}}|] = \frac{I_d}{d}. \tag{12}$$

Thence, $|\vec{\alpha}\rangle = \sum_{l=0}^{d-1} \alpha_l |l\rangle$ can be masked. □

3.2. Two-uniform quantum information masking

In this section, we focus on the case $d = 2$, leading to the simplification of the Fourier matrix to the Hadamard matrix, denoted as $F_2 = H_2$. From section 3.1, where $d \neq 2$ in F_d, we can conclude that the tensor product of $H_{2^2} = H_2 \otimes H_2$ cannot achieve QIM. Consequently, we make simple modifications to the above method to consider higher-order Hadamard matrices. To exemplify our methodology, we present a 2^3-order Hadamard matrix as an illustrative case:

$$H_{2^3} = H_{2^2} \otimes H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}. \tag{13}$$

By equation (13), the corresponding orthogonal array is

denoted by

$$\mathrm{OA}(2^3, 2^3-1, 2, 2) = \begin{pmatrix} 1&1&1&1&1&1&1\\ 0&1&0&1&0&1&0\\ 1&0&0&1&1&0&0\\ 0&0&1&1&0&0&1\\ 1&1&1&0&0&0&0\\ 0&1&0&0&1&0&1\\ 1&0&0&0&0&1&1\\ 0&0&1&0&1&1&0 \end{pmatrix} \triangleq \begin{pmatrix} \gamma_1\\ \gamma_2\\ \gamma_3\\ \gamma_4\\ \gamma_5\\ \gamma_6\\ \gamma_7\\ \gamma_{2^3} \end{pmatrix}. \tag{14}$$

The Hadamard matrix is characterized by its distinctive orthogonality property, which dictates that any two distinct rows of the matrix are orthogonal to each other. This inherent orthogonality has significant implications for the structure of the resultant orthogonal arrays. Specifically, for any given pair of such rows within an orthogonal array, there is at least one position where the corresponding elements differ.

Thus, if we consider that $\gamma_i \in \{\gamma_1, \gamma_2,\ldots,\gamma_{2^3}\}$, the quantum state generated by γ_i is denoted by $|\gamma_i\rangle$. Then, we gain

$$\langle\gamma_i|\gamma_j\rangle = 0,\ \ i, j \in \{1, 2,\cdots,2^3\},\ \ i \neq j. \tag{15}$$

To facilitate the subsequent mathematical proof, we introduce the following lemma. It is imperative to emphasize that, for the remainder of this discourse.

Lemma 2. *Let* $\mathrm{OA}(2^n, 2^n-1, 2, 2) = (\gamma_1, \gamma_2,\ldots,\gamma_{2^n})^{\mathrm{T}}$ *be an orthogonal array, then* $\langle\gamma_i|\gamma_j\rangle = 0$, *where* $n \geqslant 3$, $i,\ j \in \{1, 2,\cdots,2^n\}$ *and* $i \neq j$.

Let $|0\rangle$ and $|1\rangle$ be an orthogonal normalized basis of $\mathbb{C}^2$, and define the following physical process:

$$\begin{aligned} |1\rangle &\mapsto |\Psi_1\rangle = \sum_{i=1}^{2^n} \frac{1}{\sqrt{2^n}}|\gamma_i\rangle,\\ |0\rangle &\mapsto |\Psi_0\rangle = X^{\otimes(2^n-1)}|\Psi_1\rangle = \sum_{i=1}^{2^n} \frac{1}{\sqrt{2^n}}|\overline{\gamma}_i\rangle, \end{aligned} \tag{16}$$

where $|\overline{\gamma}_i\rangle$ indicates each element in $|\gamma_i\rangle$ is inverted, i.e., swapping 0 s for 1 s and vice versa. Thus, the following theorem is obtained.

Theorem 3. *For* $|\Psi_0\rangle$ *and* $|\Psi_1\rangle$ *generated in equation (16), there exists that all the states* $\alpha|0\rangle + \beta|1\rangle$ *can be 2-uniformly masked into* $|\Psi\rangle = \alpha|\Psi_0\rangle + \beta|\Psi_1\rangle$, *where* $|\alpha|^2 + |\beta|^2 = 1$.

The proof of **Theorem** 3 is provided in the appendix.

In **Theorem** 3, the number of qubits for the states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ is 2^n-1. The quantum states after discarding the first bit are denoted as $|\Psi_{0,1}\rangle$ and $|\Psi_{1,1}\rangle$, and this process continues until the remaining quantum states have only $2^{n-1}+3$ bits, at which point the states are denoted as $|\Psi_{0,(2^{n-1}-4)}\rangle$ and $|\Psi_{1,(2^{n-1}-4)}\rangle$. For the convenience of subsequent use, the following notation is employed.

$$\begin{aligned} &|\Psi_0\rangle \longrightarrow |\Psi_{0,1}\rangle \longrightarrow |\Psi_{0,2}\rangle \longrightarrow \cdots \longrightarrow |\Psi_{0,(2^{n-1}-4)}\rangle\\ &|\Psi_1\rangle \longrightarrow |\Psi_{1,1}\rangle \longrightarrow |\Psi_{1,2}\rangle \longrightarrow \cdots \longrightarrow |\Psi_{1,(2^{n-1}-4)}\rangle. \end{aligned} \tag{17}$$

Furthermore, based on **Theorem** 3 and above formula, we obtain that the maximum number of bits for achieving 2-uniform quantum information masking in a quantum state is 2^n-1, and the minimum is $2^{n-1}+3$. Therefore, another theorem regarding 2-uniform masking can be gained, as follows.

Theorem 4. *Let* $\{|\Psi_0\rangle, |\Psi_1\rangle\}$ *and* $\{|\Psi_{0,j}\rangle, |\Psi_{1,j}\rangle\}$ *be two pairs of quantum states that satisfy the equation (17),*

(i) for quantum states of $|\Psi_0\rangle$ and $|\Psi_1\rangle$, the original information $\alpha|0\rangle + \beta|1\rangle$ can be 2-uniformly masked into $|\Psi\rangle = \alpha|\Psi_0\rangle + \beta|\Psi_1\rangle$;

(ii) if $|\Phi_0\rangle = |\Psi_{0,j}\rangle$ and $|\Phi_1\rangle = |\Psi_{1,j}\rangle$, then $|\Psi\rangle = \alpha|\Phi_0\rangle + \beta|\Phi_1\rangle$ can achieve 2-uniform masking.

Proof. Firstly, when the number of qubits is $N = 2^n-1$, we have already proved it in **Theorem** 3. When $2^{n-1}+3 \leqslant N \leqslant 2^n-2$, that is, corresponds to the quantum states $|\Psi_{0,j}\rangle$ and $|\Psi_{1,j}\rangle$ in equation (17), where $j = 1, 2,\ldots,2^{n-1}-4$. We have

$$|\Phi_1\rangle = |\Psi_{1,j}\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=1}^{2^{n-1}} |\gamma_{i,j}\rangle(|1\rangle|\gamma_i\rangle + |0\rangle|\overline{\gamma}_i\rangle), \tag{18}$$

$$|\Phi_0\rangle = |\Psi_{0,j}\rangle = X^{\otimes N}|\Psi_{1,j}\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=1}^{2^{n-1}} |\overline{\gamma}_{i,j}\rangle(|0\rangle|\overline{\gamma}_i\rangle + |1\rangle|\gamma_i\rangle). \tag{19}$$

Given the range of values for N, it is evident that the number of bits in the quantum state $|\gamma_{i,j}\rangle$ and $|\overline{\gamma}_{i,j}\rangle$ must be greater than or equal to 2. Consequently, it is straightforward to calculate

$$\rho_{ij} = \frac{I_4}{4},\quad i,\ j \in \{1, 2,\ldots,N\},\ i \neq j. \tag{20}$$

Therefore, $|\Psi\rangle = \alpha|\Phi_0\rangle + \beta|\Phi_1\rangle$ can achieve 2-uniform masking.

When $N = 2^{n-1}+2$, quantum states have the following forms,

$$|\Psi_1'\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=1}^{2^{n-1}} |\gamma_i'\rangle(|1\rangle|\gamma_i\rangle + |0\rangle|\overline{\gamma}_i\rangle), \tag{21}$$

$$|\Psi_0'\rangle = X^{\otimes(2^{n-1}+2)}|\Psi_1'\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=1}^{2^{n-1}} |\overline{\gamma}_i'\rangle(|0\rangle|\overline{\gamma}_i\rangle + |1\rangle|\gamma_i\rangle). \tag{22}$$

It is well-known that the number of bits required to represent $|\gamma_i'\rangle$ and $|\overline{\gamma}_i'\rangle$ is 2, which can only take on the values $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. And from the basic properties of orthogonal arrays, it can be deduced that

$$\rho_{12} = \mathrm{Tr}_{34\cdots(2^{n-1}+2)}[|\Psi\rangle\langle\Psi|] = \frac{I_4}{4} + \frac{\alpha\beta^* + \alpha^*\beta}{4}X_4. \tag{23}$$

Additionally, we have

$$\rho_{ij} = \frac{I_4}{4},\ i \in \{1, 2,\ldots,2^{n-1}+2\},\ j \in \{3, 4,\ldots,2^{n-1}+2\},\ i \neq j. \tag{24}$$

Hence, $|\Psi\rangle$ cannot achieve 2-uniform masking when $N = 2^{n-1}+2$.

To sum up, only when the value range of the number of bits in the quantum state is $2^{n-1}+3 \leqslant N \leqslant 2^n - 1, |\Psi\rangle$ can achieve 2-uniform masking. The theorem has been proved. □

To provide a clearer explanation of our theorem, we present a specific example for the case when $n = 4$ below.

Example 1. For the OA $= (2^4, 2^4 - 1, 2, 2)$ in equation (A8), the corresponding 2-uniform state can be obtained, i.e.,

$$\begin{aligned}|1\rangle \mapsto |\Psi_1\rangle = \frac{1}{\sqrt{2^4}}(&|111111111111111\rangle + |010101010101010\rangle\\ &+ |100110011001100\rangle + |001100110011001\rangle\\ &+ |111000011110000\rangle + |010010110100101\rangle\\ &+ |100001111000011\rangle + |001011010010110\rangle\\ &+ |111111100000000\rangle + |010101001010101\rangle\\ &+ |100110000110011\rangle + |001100101100110\rangle\\ &+ |111000000001111\rangle + |010010101011010\rangle\\ &+ |100001100111100\rangle + |001011001101001\rangle).\end{aligned} \tag{25}$$

At the same time, we can get another 2-uniform state, namely,

$$\begin{aligned}|0\rangle \mapsto |\Psi_0\rangle &= X^{\otimes(2^4-1)}|\Psi_1\rangle\\ &= \frac{1}{\sqrt{2^4}}(|000000000000000\rangle + |101010101010101\rangle\\ &\quad + |011001100110011\rangle + |110011001100110\rangle\\ &\quad + |000111100001111\rangle + |101101001011010\rangle\\ &\quad + |011110000111100\rangle + |110100101101001\rangle\\ &\quad + |000000011111111\rangle + |101010110101010\rangle\\ &\quad + |011001111001100\rangle + |110011010011001\rangle\\ &\quad + |000111111110000\rangle + |101101010100101\rangle\\ &\quad + |011110011000011\rangle + |110100110010110\rangle).\end{aligned} \tag{26}$$

The general qubit state $\alpha|0\rangle + \beta|1\rangle$ is masked as $|\Psi\rangle = \alpha|\Psi_0\rangle + \beta|\Psi_1\rangle$. Through equations (25) and (26), we calculate that

$$\rho_{ij} = \frac{I_4}{4},\quad i,\ j \in \{1, 2,\ldots,2^4 - 1\},\ i \neq j. \tag{27}$$

Therefore, when $N = 2^4 - 1$, all the qubit states can be 2-uniformly masked.

Removing some qubits from $|\Psi_0\rangle$ and $|\Psi_1\rangle$, respectively, yields the following quantum states. In this case, $N = 2^{4-1}+3$ is the minimum number of quantum states required for achieving QIM.

$$\begin{aligned}|1\rangle \mapsto |\Psi_{1,4}\rangle = \frac{1}{\sqrt{2^4}}(&|111111111111\rangle + |010101010101\rangle\\ &+ |100110011001\rangle + |001100110011001\rangle\\ &+ |000111100000\rangle + |101101001010110\rangle\\ &+ |011110000011\rangle + |110100101010110\rangle\\ &+ |111000000000\rangle + |010010101010101\rangle\\ &+ |100001100110011\rangle + |001011001100110\rangle\\ &+ |000000011111\rangle + |101010110101010\rangle\\ &+ |011001111001100\rangle + |110011001001001\rangle).\end{aligned} \tag{28}$$

$$\begin{aligned}|0\rangle \mapsto |\Psi_{0,4}\rangle &= X^{\otimes(2^{4-1}+3)}|\Psi_{1,4}\rangle\\ &= \frac{1}{\sqrt{2^4}}(|000000000000\rangle + |101010101010101\rangle\\ &\quad + |011001100110011\rangle + |110011001100110\rangle\\ &\quad + |111000011110000\rangle + |010010110100101\rangle\\ &\quad + |100001111000011\rangle + |001011010010110\rangle\\ &\quad + |000111111111\rangle + |101101010101010\rangle\\ &\quad + |011110011000011\rangle + |110100110010110\rangle\\ &\quad + |100110000011\rangle + |001100101100110\rangle).\end{aligned} \tag{29}$$

And the following partial trace is gained,

$$\rho_{ij} = \frac{I_4}{4},\quad i,\ j \in \{1, 2,\ldots,2^4 - 5\},\ i \neq j. \tag{30}$$

Therefore, regardless of how the two parameters of α, β are selected, when $n = 4$, the quantum state range within $2^{4-1}+3 \leqslant N \leqslant 2^4 - 1, |\Psi\rangle$ can achieve 2-uniform masking.

For every quantum state $|\Psi\rangle$, we can show the corresponding quantum circuit diagram. For example, consider the quantum state $|\Psi\rangle = \alpha|\Psi_{0,4}\rangle + \beta|\Psi_{1,4}\rangle$, as shown in figure 1.

4. Application of quantum information masking

Quantum information masking forms the basis for quantum secret sharing, where legitimate participants can recover the original quantum state through collaboration, while unauthorized ones cannot. Therefore, Alice encodes the original information $\alpha|0\rangle + \beta|1\rangle$ into a multipartite quantum state $|\Psi\rangle = \alpha|\Psi_0\rangle + \beta|\Psi_1\rangle$, and then distributes each particle of $|\Psi\rangle$ to each participant. We term the stage of recovering the secret with minimal participants as the secret recovery phase. In this section, to highlight the applicability of the quantum states, we will explore how to recover the secret using the state $|\Psi\rangle = \alpha|\Psi_{0,4}\rangle + \beta|\Psi_{1,4}\rangle$ as shown in Example 1.

Alice prepares the quantum state $|\Psi\rangle$ and sends each particle to each participant via a decoy photon sequence.

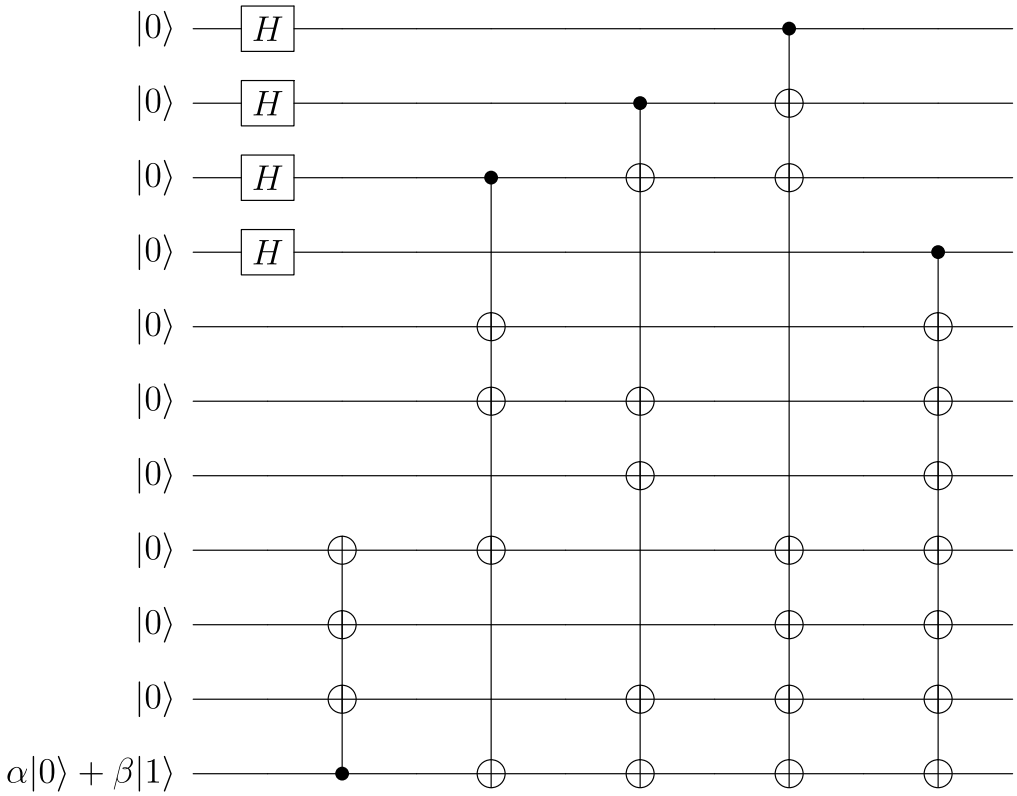

Figure 1. Quantum circuit diagram for generating $|\Psi\rangle$ state.

These participants can be denoted by P_1, P_2, …, P_{11}. During the recovery process, we omitted the coefficient of $|\Psi_{0,4}\rangle$ and $|\Psi_{1,4}\rangle$ as they do not affect the final result.

In addition, we consider the structure of the legitimate participants as shown in figure 2, where the structure can be represented as

$$\begin{aligned}\Gamma = \{&\{P_1, P_2, P_3, P_4, P_5, P_6, P_8\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_6, P_9\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_6, P_{10}\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_6, P_{11}\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_7, P_8\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_7, P_9\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_7, P_{10}\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_7, P_{11}\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_8, P_{10}\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_8, P_{11}\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_9, P_{10}\},\\ &\{P_1, P_2, P_3, P_4, P_5, P_9, P_{11}\}\}. \end{aligned} \tag{31}$$

In figure 2, we present all sets of participants that can recover secrets. Furthermore, we take the set P_1, P_2, P_3, P_4, P_5, P_6, P_8 as an example. Other situations can be similarly analyzed.

Step 1. The participant P_4 carries out several measurements on his particle in $|\Psi\rangle$ under the basis of $\{|0\rangle, |1\rangle\}$. At the same time, the remaining participants can get the following collapse states on their own particles.

(1) If the measurement by P_4 is $|0\rangle$, then the quantum state $|\Psi\rangle$ can collapse to $|\tilde{\phi}_0\rangle$, where $|\tilde{\phi}_0\rangle$ is denoted by

$$\begin{aligned}|\tilde{\phi}_0\rangle = &(\alpha\,|000\rangle + \beta|111\rangle)_{123}|00000000\rangle\\ &+ (\alpha\,|101\rangle + \beta|010\rangle)_{123}|01010101\rangle\\ &+ (\alpha\,|011\rangle + \beta|100\rangle)_{123}|00110011\rangle\\ &+ (\alpha\,|110\rangle + \beta|001\rangle)_{123}|01100110\rangle\\ &+ (\alpha\,|111\rangle + \beta|000\rangle)_{123}|00001111\rangle\\ &+ (\alpha\,|010\rangle + \beta|101\rangle)_{123}|01011010\rangle\\ &+ (\alpha\,|100\rangle + \beta|011\rangle)_{123}|00111100\rangle\\ &+ (\alpha\,|001\rangle + \beta|110\rangle)_{123}|01101001\rangle. \end{aligned} \tag{32}$$

(2) If the measurement by P_4 is $|1\rangle$, then the quantum state $|\Psi\rangle$ can collapse to $|\tilde{\phi}_1\rangle$, where $|\tilde{\phi}_1\rangle$ is denoted by

$$\begin{aligned}|\tilde{\phi}_1\rangle = &(\alpha\,|000\rangle + \beta|111\rangle)_{123}|11111111\rangle\\ &+ (\alpha\,|101\rangle + \beta|010\rangle)_{123}|10101010\rangle\\ &+ (\alpha\,|011\rangle + \beta|100\rangle)_{123}|11001100\rangle\\ &+ (\alpha\,|110\rangle + \beta|001\rangle)_{123}|10011001\rangle\\ &+ (\alpha\,|111\rangle + \beta|000\rangle)_{123}|11110000\rangle\\ &+ (\alpha\,|010\rangle + \beta|101\rangle)_{123}|10100101\rangle\\ &+ (\alpha\,|100\rangle + \beta|011\rangle)_{123}|11000011\rangle\\ &+ (\alpha\,|001\rangle + \beta|110\rangle)_{123}|10010110\rangle. \end{aligned} \tag{33}$$

Step 2. The participant P_5 measures the quantum state $|\tilde{\phi}_0\rangle$ or $|\tilde{\phi}_1\rangle$ with a computational basis $\{|0\rangle, |1\rangle\}$. Then, he can

obtain four cases, namely, four quantum states are collapsed into

$$\begin{aligned}|\tilde{\phi}_{00}\rangle = &(\alpha\,|000\rangle + \beta|111\rangle)_{123}|00000000\rangle\\ &+ (\alpha\,|011\rangle + \beta|100\rangle)_{123}|00110011\rangle\\ &+ (\alpha\,|111\rangle + \beta|000\rangle)_{123}|00001111\rangle\\ &+ (\alpha\,|100\rangle + \beta|011\rangle)_{123}|00111100\rangle, \end{aligned} \tag{34}$$

$$\begin{aligned}|\tilde{\phi}_{01}\rangle = &(\alpha\,|101\rangle + \beta|010\rangle)_{123}|01010101\rangle\\ &+ (\alpha\,|110\rangle + \beta|001\rangle)_{123}|01100110\rangle\\ &+ (\alpha\,|010\rangle + \beta|101\rangle)_{123}|01011010\rangle\\ &+ (\alpha\,|001\rangle + \beta|110\rangle)_{123}|01101001\rangle, \end{aligned} \tag{35}$$

$$\begin{aligned}|\tilde{\phi}_{10}\rangle = &(\alpha\,|101\rangle + \beta|010\rangle)_{123}|10101010\rangle\\ &+ (\alpha\,|110\rangle + \beta|001\rangle)_{123}|10011001\rangle\\ &+ (\alpha\,|010\rangle + \beta|101\rangle)_{123}|10100101\rangle\\ &+ (\alpha\,|001\rangle + \beta|110\rangle)_{123}|10010110\rangle, \end{aligned} \tag{36}$$

$$\begin{aligned}|\tilde{\phi}_{11}\rangle = &(\alpha\,|000\rangle + \beta|111\rangle)_{123}|11111111\rangle\\ &+ (\alpha\,|011\rangle + \beta|100\rangle)_{123}|11001100\rangle\\ &+ (\alpha\,|111\rangle + \beta|000\rangle)_{123}|11110000\rangle\\ &+ (\alpha\,|100\rangle + \beta|011\rangle)_{123}|11000011\rangle. \end{aligned} \tag{37}$$

Step 3. P_6 and P_8 use $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ to measure their particles of $|\tilde{\phi}_{00}\rangle$, $|\tilde{\phi}_{01}\rangle$, $|\tilde{\phi}_{10}\rangle$ or $|\tilde{\phi}_{11}\rangle$. These states obtained after measurement are as follows,

$$\begin{aligned}
|\tilde{\phi}_{0000}\rangle &= (\alpha|000\rangle + \beta|111\rangle)_{123}|00000000\rangle,\\
|\tilde{\phi}_{0001}\rangle &= (\alpha|111\rangle + \beta|000\rangle)_{123}|00001111\rangle,\\
|\tilde{\phi}_{0010}\rangle &= (\alpha|011\rangle + \beta|100\rangle)_{123}|00110011\rangle,\\
|\tilde{\phi}_{0011}\rangle &= (\alpha|100\rangle + \beta|011\rangle)_{123}|00111100\rangle,\\
|\tilde{\phi}_{0100}\rangle &= (\alpha|101\rangle + \beta|010\rangle)_{123}|01010101\rangle,\\
|\tilde{\phi}_{0101}\rangle &= (\alpha|010\rangle + \beta|101\rangle)_{123}|01011010\rangle,\\
|\tilde{\phi}_{0110}\rangle &= (\alpha|110\rangle + \beta|001\rangle)_{123}|01100110\rangle,\\
|\tilde{\phi}_{0111}\rangle &= (\alpha|001\rangle + \beta|110\rangle)_{123}|01101001\rangle,\\
|\tilde{\phi}_{1000}\rangle &= (\alpha|001\rangle + \beta|110\rangle)_{123}|10010110\rangle,\\
|\tilde{\phi}_{1001}\rangle &= (\alpha|110\rangle + \beta|001\rangle)_{123}|10011001\rangle,\\
|\tilde{\phi}_{1010}\rangle &= (\alpha|010\rangle + \beta|101\rangle)_{123}|10100101\rangle,\\
|\tilde{\phi}_{1011}\rangle &= (\alpha|101\rangle + \beta|010\rangle)_{123}|10101010\rangle,\\
|\tilde{\phi}_{1100}\rangle &= (\alpha|100\rangle + \beta|011\rangle)_{123}|11000011\rangle,\\
|\tilde{\phi}_{1101}\rangle &= (\alpha|011\rangle + \beta|100\rangle)_{123}|11001100\rangle,\\
|\tilde{\phi}_{1110}\rangle &= (\alpha|111\rangle + \beta|000\rangle)_{123}|11110000\rangle,\\
|\tilde{\phi}_{1111}\rangle &= (\alpha|000\rangle + \beta|111\rangle)_{123}|11111111\rangle.
\end{aligned} \tag{38}$$

Step 4. These participants, $\{P_1, P_2, P_3\}$, cooperate to use a Controlled-NOT gate on their particles with the first qubit as the control and the second and third qubits as target bits. Then, the above states in equation (38) yields the following states,

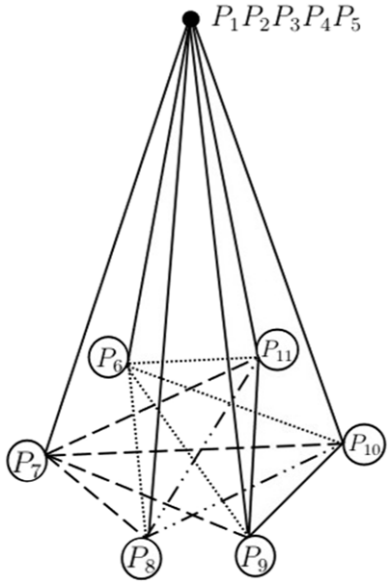

Figure 2. Schematic of seven participants collaborating to recover secrets, where each triangle formed by connecting vertex $P_1P_2P_3P_4P_5$ with any two endpoints of the edges below represents a valid secret recovery set.

$$\begin{aligned}
|\phi_{0000}\rangle &= (\alpha|0\rangle + \beta|1\rangle)_1|0000000000\rangle,\\
|\phi_{0001}\rangle &= (\alpha|1\rangle + \beta|0\rangle)_1|0000001111\rangle,\\
|\phi_{0010}\rangle &= (\alpha|0\rangle + \beta|1\rangle)_1|1100110011\rangle,\\
|\phi_{0011}\rangle &= (\alpha|1\rangle + \beta|0\rangle)_1|1100111100\rangle,\\
|\phi_{0100}\rangle &= (\alpha|1\rangle + \beta|0\rangle)_1|1001010101\rangle,\\
|\phi_{0101}\rangle &= (\alpha|0\rangle + \beta|1\rangle)_1|1001011010\rangle,\\
|\phi_{0110}\rangle &= (\alpha|1\rangle + \beta|0\rangle)_1|0101100110\rangle,\\
|\phi_{0111}\rangle &= (\alpha|0\rangle + \beta|1\rangle)_1|0101101001\rangle,\\
|\phi_{1000}\rangle &= (\alpha|0\rangle + \beta|1\rangle)_1|0110010110\rangle,\\
|\phi_{1001}\rangle &= (\alpha|1\rangle + \beta|0\rangle)_1|0110011001\rangle,\\
|\phi_{1010}\rangle &= (\alpha|0\rangle + \beta|1\rangle)_1|1010100101\rangle,\\
|\phi_{1011}\rangle &= (\alpha|1\rangle + \beta|0\rangle)_1|1010101010\rangle,\\
|\phi_{1100}\rangle &= (\alpha|1\rangle + \beta|0\rangle)_1|1111000011\rangle,\\
|\phi_{1101}\rangle &= (\alpha|0\rangle + \beta|1\rangle)_1|1111001100\rangle,\\
|\phi_{1110}\rangle &= (\alpha|1\rangle + \beta|0\rangle)_1|0011110000\rangle,\\
|\phi_{1111}\rangle &= (\alpha|0\rangle + \beta|1\rangle)_1|0011111111\rangle.
\end{aligned} \tag{39}$$

Step 5. According to the measurements of the four participants P_4, P_5, P_6, P_8, P_1 performs the following operations, as shown in table 1. Therefore, P_1 can recover the original quantum state $\alpha|0\rangle + \beta|1\rangle$.

5. Conclusion

In this paper, we introduced a framework for 1-uniform quantum information masking in multipartite systems, facilitated by the application of a Fourier matrix. Furthermore, we constructed an orthogonal array utilizing a specialized Fourier matrix, which we then leverage to develop a methodology for the implementation of 2-uniform quantum information

Table 1. The operations to recover the secret executed by $P_1P_2P_3P_4P_5P_6P_8$, where I represents the identical operation and X represents the bit flip operation.

Measurement result by $P_4P_5P_6P_8$	Collapsed states after measurement	States after using a CNOT gate with $P_1P_2P_3$	Operations performed by P_1
$\|0000\rangle$	$\|\tilde{\phi}_{0000}\rangle$	$\|\phi_{0000}\rangle$	I
$\|0001\rangle$	$\|\tilde{\phi}_{0001}\rangle$	$\|\phi_{0001}\rangle$	X
$\|0010\rangle$	$\|\tilde{\phi}_{0010}\rangle$	$\|\phi_{0010}\rangle$	I
$\|0011\rangle$	$\|\tilde{\phi}_{0011}\rangle$	$\|\phi_{0011}\rangle$	X
$\|0100\rangle$	$\|\tilde{\phi}_{0100}\rangle$	$\|\phi_{0100}\rangle$	X
$\|0101\rangle$	$\|\tilde{\phi}_{0101}\rangle$	$\|\phi_{0101}\rangle$	I
$\|0110\rangle$	$\|\tilde{\phi}_{0110}\rangle$	$\|\phi_{0110}\rangle$	X
$\|0111\rangle$	$\|\tilde{\phi}_{0111}\rangle$	$\|\phi_{0111}\rangle$	I
$\|1000\rangle$	$\|\tilde{\phi}_{1000}\rangle$	$\|\phi_{1000}\rangle$	I
$\|1001\rangle$	$\|\tilde{\phi}_{1001}\rangle$	$\|\phi_{1001}\rangle$	X
$\|1010\rangle$	$\|\tilde{\phi}_{1010}\rangle$	$\|\phi_{1010}\rangle$	I
$\|1011\rangle$	$\|\tilde{\phi}_{1011}\rangle$	$\|\phi_{1011}\rangle$	X
$\|1100\rangle$	$\|\tilde{\phi}_{1100}\rangle$	$\|\phi_{1100}\rangle$	X
$\|1101\rangle$	$\|\tilde{\phi}_{1101}\rangle$	$\|\phi_{1101}\rangle$	I
$\|1110\rangle$	$\|\tilde{\phi}_{1110}\rangle$	$\|\phi_{1110}\rangle$	X
$\|1111\rangle$	$\|\tilde{\phi}_{1111}\rangle$	$\|\phi_{1111}\rangle$	I

masking. Subsequently, we generated two 2-uniform states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ based on the corresponding orthogonal array. Next, we proceeded to demonstrate that a quantum state $|\Psi\rangle = \alpha|\Psi_0\rangle + \beta|\Psi_1\rangle$ can mask the quantum state into multipartite systems. Moreover, if the number of qubits for $|\Psi_0\rangle$ and $|\Psi_1\rangle$ decreased sequentially from left to right, and the count N satisfies the condition $2^{n-1}+3 \leqslant N \leqslant 2^n - 1$, $|\Psi\rangle$ could also achieve 2-uniform masking. To illustrate our method, we presented a quantum circuit diagram for generating $|\Psi\rangle$ when $n = 4$. Finally, to prove that our scheme can be applied to quantum secret sharing, we also provided a specific application of 2-uniform quantum information masking.

Acknowledgments

We want to express our gratitude to anonymous referees for their valuable and constructive comments. This work is supported by the National Natural Science Foundation of China under Grant No. 12301590 and the Natural Science Foundation of Hebei Province under Grant No. A2022210002.

Appendix: The proof of theorem 3.

Proof. Firstly, when $n = 3$ and $N = 2^3 - 1$, the following 2-uniform quantum state can be obtained from the orthogonal array of equation (14),

$$\begin{aligned}|1\rangle \mapsto |\Psi_1^{2^3}\rangle &= \frac{1}{\sqrt{2^3}}(|1111111\rangle + |0101010\rangle \\ &\quad + |1001100\rangle + |0011001\rangle \\ &\quad + |1110000\rangle + |0100101\rangle \\ &\quad + |1000011\rangle + |0010110\rangle) \\ &= \sum_{i=1}^{2^3} \frac{1}{\sqrt{2^3}}|\gamma_i\rangle. \end{aligned} \tag{A1}$$

Based on **Lemma** 2, we have $\langle\gamma_i|\gamma_j\rangle = 0$, $i, j \in \{1, 2,\ldots,2^3\}$, $i \neq j$. Furthermore, another 2-uniform quantum state can be obtained, namely,

$$\begin{aligned}|0\rangle \mapsto |\Psi_0^{2^3}\rangle &= X^{\otimes(2^3-1)}|\Psi_1^{2^3}\rangle \\ &= \frac{1}{\sqrt{2^3}}(|0000000\rangle + |1010101\rangle \\ &\quad + |0110011\rangle + |1100110\rangle \\ &\quad + |0001111\rangle + |1011010\rangle \\ &\quad + |0111100\rangle + |1101001\rangle) \\ &= \sum_{i=1}^{2^3} \frac{1}{\sqrt{2^3}}|\overline{\gamma}_i\rangle. \end{aligned} \tag{A2}$$

Similarly, it is easy to get $\langle\overline{\gamma}_i|\overline{\gamma}_j\rangle = 0$, $i, j \in \{1, 2,\ldots,2^3\}$ and $i \neq j$.

Utilizing the inherent characteristics of the orthogonal array, the first two bits of each quantum state can be extracted and obtained, namely,

$$\begin{aligned}|\Psi_1^{2^3}\rangle &= \frac{1}{\sqrt{2^3}}(|11\rangle|11111\rangle + |01\rangle|01010\rangle \\ &\quad + |10\rangle|01100\rangle + |00\rangle|11001\rangle \\ &\quad + |11\rangle|10000\rangle + |01\rangle|00101\rangle \\ &\quad + |10\rangle|00011\rangle + |00\rangle|10110\rangle) \\ &\triangleq \frac{1}{\sqrt{2^3}}(|11\rangle(|\delta_1\rangle + |\delta_2\rangle) + |01\rangle(|\delta_3\rangle + |\delta_4\rangle) \\ &\quad + |10\rangle(|\delta_5\rangle + |\delta_6\rangle) + |11\rangle(|\delta_7\rangle + |\delta_8\rangle)), \end{aligned} \tag{A3}$$

$$\begin{aligned}|\Psi_0^{2^3}\rangle &= \frac{1}{\sqrt{2^3}}(|00\rangle|00000\rangle + |10\rangle|10101\rangle \\ &\quad + |01\rangle|10011\rangle + |11\rangle|00110\rangle \\ &\quad + |00\rangle|01111\rangle + |10\rangle|11010\rangle \\ &\quad + |01\rangle|11100\rangle + |11\rangle|01001\rangle) \\ &\triangleq \frac{1}{\sqrt{2^3}}(|00\rangle(|\overline{\delta}_1\rangle + |\overline{\delta}_2\rangle) + |10\rangle(|\overline{\delta}_3\rangle + |\overline{\delta}_4\rangle) \\ &\quad + |01\rangle(|\overline{\delta}_5\rangle + |\overline{\delta}_6\rangle) + |00\rangle(|\overline{\delta}_7\rangle + |\overline{\delta}_8\rangle)), \end{aligned} \tag{A4}$$

where $\langle\delta_i|\delta_j\rangle = 0$, $\langle\overline{\delta}_i|\overline{\delta}_j\rangle = 0$, $\langle\delta_i|\overline{\delta}_i\rangle = 0$, $\langle\overline{\delta}_i|\delta_i\rangle = 0$, $i, j \in \{1, 2,\ldots,2^3\}$, $i \neq j$.

Therefore, for $|\Psi\rangle = \alpha|\Psi_0^{2^3}\rangle + \beta|\Psi_1^{2^3}\rangle (|\alpha|^2 + |\beta|^2 = 1)$, tracing out the 3, 4,$\cdots$,$(2^3 - 1)$ qubits, we find the reduced

density operator of the first and the second qubits,

$$\rho_{12} = \mathrm{Tr}_{34\cdots(2^3-1)}[|\Psi\rangle\langle\Psi|] = \frac{I_4}{4}. \tag{A5}$$

From the arbitrariness of orthogonal arrays, it can be inferred that

$$\rho_{ij} = \frac{I_4}{4}, \quad i,\ j \in \{1, 2,\ldots,2^3 - 1\},\ i \neq j. \tag{A6}$$

Thus, when $n = 3$, all the quantum states $\alpha|0\rangle + \beta|1\rangle$ can be 2-uniformly masked into $|\Psi\rangle = \alpha|\Psi_0^{2^3}\rangle + \beta|\Psi_1^{2^3}\rangle$.

Next, consider when $n = 4$ and $N = 2^4 - 1$. According to the general formula of the Hadamard matrix,

$$H_{2^4} = H_{2^3} \otimes H_2 = \begin{pmatrix} H_{2^3} & H_{2^3} \\ H_{2^3} & -H_{2^3} \end{pmatrix}. \tag{A7}$$

It is easy to obtain that

$$\mathrm{OA}(2^4,\ 2^4 - 1,\ 2,\ 2) = \left(\begin{array}{c|cc} \gamma_1 & 1 & \gamma_1 \\ \gamma_2 & 1 & \gamma_2 \\ \vdots & \vdots & \vdots \\ \gamma_{2^3} & 1 & \gamma_{2^3} \\ \hline \gamma_1 & 0 & \overline{\gamma}_1 \\ \gamma_2 & 0 & \overline{\gamma}_2 \\ \vdots & \vdots & \vdots \\ \gamma_{2^3} & 0 & \overline{\gamma}_{2^3} \end{array}\right). \tag{A8}$$

Accordingly, two 2-uniform quantum states can be gained, denoted as

$$|\Psi_1^{2^4}\rangle = \frac{1}{\sqrt{2^4}}\sum_{i=1}^{2^3}|\gamma_i\rangle(|1\rangle|\gamma_i\rangle + |0\rangle|\overline{\gamma}_i\rangle), \tag{A9}$$

$$|\Psi_0^{2^4}\rangle = X^{\otimes(2^4-1)}|\Psi_1^{2^4}\rangle = \frac{1}{\sqrt{2^4}}\sum_{i=1}^{2^3}|\overline{\gamma}_i\rangle(|0\rangle|\overline{\gamma}_i\rangle + |1\rangle|\gamma_i\rangle). \tag{A10}$$

As a consequence,

$$\begin{aligned} |\Psi\rangle &= \alpha|\Psi_0^{2^4}\rangle + \beta|\Psi_1^{2^4}\rangle \\ &= \frac{1}{\sqrt{2^4}}\sum_{i=1}^{2^3}[\alpha(|\overline{\gamma}_i\rangle|0\rangle|\overline{\gamma}_i\rangle + |\overline{\gamma}_i\rangle|1\rangle|\gamma_i\rangle) \\ &\quad + \beta(|\gamma_i\rangle|1\rangle|\gamma_i\rangle + |\gamma_i\rangle|0\rangle|\overline{\gamma}_i\rangle)], \end{aligned} \tag{A11}$$

where $|\overline{\gamma}_i\rangle|0\rangle|\overline{\gamma}_i\rangle$, $|\overline{\gamma}_i\rangle|1\rangle|\gamma_i\rangle$, $|\gamma_i\rangle|1\rangle|\gamma_i\rangle$ and $|\gamma_i\rangle|0\rangle|\overline{\gamma}_i\rangle$ are quantum states generated by each row of $\mathrm{OA}(2^4,\ 2^4 - 1,\ 2,\ 2)$.

Based on the basic properties of orthogonal array, the first two qubits of each quantum state in $|\Psi\rangle$ can be extracted, resulting in the following form

$$\begin{aligned} |\Psi\rangle = \frac{1}{\sqrt{2^4}}[&\alpha(|00\rangle(|\zeta_1\rangle + |\zeta_2\rangle + |\zeta_3\rangle + |\zeta_4\rangle) \\ &+ |10\rangle(|\zeta_5\rangle + |\zeta_6\rangle + |\zeta_7\rangle + |\zeta_8\rangle) \\ &+ |01\rangle(|\zeta_9\rangle + |\zeta_{10}\rangle + |\zeta_{11}\rangle + |\zeta_{12}\rangle) \\ &+ |11\rangle(|\zeta_{13}\rangle + |\zeta_{14}\rangle + |\zeta_{15}\rangle + |\zeta_{16}\rangle)) \\ &+ \beta(|11\rangle(|\overline{\zeta}_1\rangle + |\overline{\zeta}_2\rangle + |\overline{\zeta}_3\rangle + |\overline{\zeta}_4\rangle) \\ &+ |01\rangle(|\overline{\zeta}_5\rangle + |\overline{\zeta}_6\rangle + |\overline{\zeta}_7\rangle + |\overline{\zeta}_8\rangle) \\ &+ |10\rangle(|\overline{\zeta}_9\rangle + |\overline{\zeta}_{10}\rangle + |\overline{\zeta}_{11}\rangle + |\overline{\zeta}_{12}\rangle) \\ &+ |00\rangle(|\overline{\zeta}_{13}\rangle + |\overline{\zeta}_{14}\rangle + |\overline{\zeta}_{15}\rangle + |\overline{\zeta}_{16}\rangle))], \end{aligned} \tag{A12}$$

where $\langle\zeta_i|\zeta_j\rangle = 0$, $\langle\overline{\zeta}_i|\overline{\zeta}_j\rangle = 0$, $\langle\zeta_i|\overline{\zeta}_i\rangle = 0$, $\langle\overline{\zeta}_i|\zeta_i\rangle = 0$, $i,\ j \in \{1, 2,\ldots,2^4\}$ and $i \neq j$.

It is easy to calculate that

$$\rho_{12} = \mathrm{Tr}_{34\cdots(2^4-1)}[|\Psi\rangle\langle\Psi|] = \frac{I_4}{4}. \tag{A13}$$

And due to the arbitrariness of the basic properties of orthogonal arrays, there is

$$\rho_{ij} = \frac{I_4}{4}, \quad i,\ j \in \{1, 2,\ldots,2^4 - 1\},\ i \neq j. \tag{A14}$$

As a result, when $n = 4$, all the quantum states $\alpha|0\rangle + \beta|1\rangle$ can be 2-uniformly masked into $|\Psi\rangle = \alpha|\Psi_0^{2^4}\rangle + \beta|\Psi_1^{2^4}\rangle$.

Suppose that $n = m$ and $N = 2^m - 1$, $\alpha|0\rangle + \beta|1\rangle$ can also be 2-uniformly masked into $|\Psi\rangle = \alpha|\Psi_0^{2^m}\rangle + \beta|\Psi_1^{2^m}\rangle$. Below, we will focus solely on the case where $n = m + 1$ and $N = 2^{m+1} - 1$.

For convenience, the orthogonal array corresponding to H_{2^m} can be denoted as

$$\mathrm{OA}(2^m,\ 2^m - 1,\ 2,\ 2) = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_{2^m} \end{pmatrix}, \tag{A15}$$

where $\langle\gamma_i|\gamma_j\rangle = 0$, $i,\ j \in \{1, 2,\ldots,2^m\}$ and $i \neq j$.

Therefore, the orthogonal array corresponding to $H_{2^{m+1}}$ can be represented as

$$\mathrm{OA}(2^{m+1},\ 2^{m+1} - 1,\ 2,\ 2) = \left(\begin{array}{c|cc} \gamma_1 & 1 & \gamma_1 \\ \gamma_2 & 1 & \gamma_2 \\ \vdots & \vdots & \vdots \\ \gamma_{2^m} & 1 & \gamma_{2^m} \\ \hline \gamma_1 & 0 & \overline{\gamma}_1 \\ \gamma_2 & 0 & \overline{\gamma}_2 \\ \vdots & \vdots & \vdots \\ \gamma_{2^m} & 0 & \overline{\gamma}_{2^m} \end{array}\right). \tag{A16}$$

So, the generated 2-uniform states are

$$|\Psi_1^{2^{m+1}}\rangle = \frac{1}{\sqrt{2^{m+1}}}\sum_{i=1}^{2^m}|\gamma_i\rangle(|1\rangle|\gamma_i\rangle + |0\rangle|\overline{\gamma}_i\rangle), \tag{A17}$$

$$|\Psi_0^{2^{m+1}}\rangle = X^{\otimes(2^{m+1}-1)}|\Psi_1^{2^{m+1}}\rangle$$
$$= \frac{1}{\sqrt{2^{m+1}}}\sum_{i=1}^{2^m}|\overline{\gamma_i}\rangle(|0\rangle|\overline{\gamma_i}\rangle + |1\rangle|\gamma_i\rangle). \quad \text{(A18)}$$

As a consequence,

$$|\Psi\rangle = \alpha|\Psi_0^{2^{m+1}}\rangle + \beta|\Psi_1^{2^{m+1}}\rangle$$
$$= \frac{1}{\sqrt{2^{m+1}}}\sum_{i=1}^{2^m}[\alpha(|\overline{\gamma_i}\rangle|0\rangle|\overline{\gamma_i}\rangle + |\overline{\gamma_i}\rangle|1\rangle|\gamma_i\rangle)$$
$$+ \beta(|\gamma_i\rangle|1\rangle|\gamma_i\rangle + |\gamma_i\rangle|0\rangle|\overline{\gamma_i}\rangle)], \quad \text{(A19)}$$

where $|\overline{\gamma_i}\rangle|0\rangle|\overline{\gamma_i}\rangle$, $|\overline{\gamma_i}\rangle|1\rangle|\gamma_i\rangle$, $|\gamma_i\rangle|1\rangle|\gamma_i\rangle$ and $|\gamma_i\rangle|0\rangle|\overline{\gamma_i}\rangle$ are quantum states generated by each row of OA(2^{m+1}, $2^{m+1}-1$, 2, 2).

Therefore, by **Lemma** 2, we know that they are pairwise orthogonal. In addition, based on the properties of orthogonal array, the first two qubits of each quantum state in $|\Psi\rangle$ can be extracted, as follow,

$$|\Psi\rangle = \frac{1}{\sqrt{2^{m+1}}}\left[\sum_{i=1}^{2^{m-1}}(\alpha|00\rangle|\xi_i\rangle + \beta|11\rangle|\overline{\xi}_i\rangle)\right.$$
$$+ \sum_{i=2^{m-1}+1}^{2^m}(\alpha|10\rangle|\xi_i\rangle + \beta|01\rangle|\overline{\xi}_i\rangle)$$
$$+ \sum_{i=2^m+1}^{2^m+2^{m-1}}(\alpha|01\rangle|\xi_i\rangle + \beta|10\rangle|\overline{\xi}_i\rangle)$$
$$\left.+ \sum_{i=2^m+2^{m-1}+1}^{2^{m+1}}(\alpha|11\rangle|\xi_i\rangle + \beta|00\rangle|\overline{\xi}_i\rangle)\right], \quad \text{(A20)}$$

where $\langle\xi_i|\xi_j\rangle = 0$, $\langle\overline{\xi}_i|\overline{\xi}_j\rangle = 0$, $\langle\xi_i|\overline{\xi}_i\rangle = 0$, $\langle\overline{\xi}_i|\xi_i\rangle = 0$, $i, j \in \{1, 2, \ldots, 2^{m+1}\}$, $i \neq j$.

We calculate that

$$\rho_{12} = \mathrm{Tr}_{34\cdots(2^{m+1}-1)}[|\Psi\rangle\langle\Psi|] = \frac{I_4}{4}. \quad \text{(A21)}$$

Since the arbitrariness of the orthogonal array, it is easy to verify that

$$\rho_{ij} = \frac{I_4}{4}, \quad i, j \in \{1, 2, \ldots, 2^{m+1}-1\}, \ i \neq j. \quad \text{(A22)}$$

Thus, all the quantum states $\alpha|0\rangle + \beta|1\rangle$ can be 2-uniformly masked into $|\Psi\rangle = \alpha|\Psi_0\rangle + \beta|\Psi_1\rangle$. This completes the proof. □

References

[1] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802
[2] Dieks D 1982 Overlap and distinguishability of quantum states *Phys. Lett.* A **92** 271
[3] Yuen H P 1986 Amplification of quantum states and noiseless photon amplifiers *Phys. Lett.* A **113** 405
[4] Pati A K and Braunstein S L 2000 Impossibility of deleting an unknown quantunm state *Nature* **404** 164
[5] Braunstein S L and Pati A K 2007 Quantum information cannot be completely hidden in correlations: implications for the black-hole information paradox *Phys. Rev. Lett.* **98** 080502
[6] Girling M, Cîrstoiu C and Jennings D 2024 Simple formulation of no-cloning and no-hiding that admits efficient and robust verification *Phys. Rev. Res.* **6** 023090
[7] Kalev A and Hen I 2008 No-broadcasting theorem and its classical counterpart *Phys. Rev. Lett.* **100** 210502
[8] Heinosaari T, Jenčová A and Plávala M 2023 Dispensing of quantum information beyond nobroadcasting theorem is it possible to broadcast anything genuinely quantum *J. Phys. A: Math. Theor.* **56** 135301
[9] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865
[10] Grünenfelder F *et al* 2023 Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems *Nat. Photon.* **17** 422–6
[11] Bouwmeester D *et al* 1997 Experimental quantum teleportation *Nature* **390** 575
[12] Hermans L N *et al* 2022 Qubit teleportation between nonneighbouring nodes in a quantum network *Nature* **605** 663–8
[13] Hillery M, Bužek V and Berthiaume A 1999 Quantum secret sharing *Phys. Rev.* A **59** 1829
[14] Senthoor K and Sarvepalli P K 2022 Theory of communication efficient quantum secret sharing *IEEE Trans. Inf. Theory* **68** 3164–86
[15] Singh P and Chakrabarty I 2024 Controlled state reconstruction and quantum secret sharing *Phys. Rev.* A **109** 032406
[16] Bai C M, Zhang S J and Liu L 2022 Quantum secret sharing based on quantum information masking *Quantum Inf. Process.* **21** 377
[17] Modi K, Pati A K, Sen(De) A and Sen U 2018 Masking quantum information is impossible *Phys. Rev. Lett.* **120** 230501
[18] Li M S and Wang Y L 2018 Masking quantum information in multipartite scenario *Phys. Rev.* A **98** 062306
[19] Wang M Y, Zhang S J, Bai C M and Liu L 2022 The masking condition for the quantum state in two-dimensional Hilbert space *Commun. Theor. Phys.* **74** 115101
[20] Wang Q, Zhang S J, Bai C M and Liu L 2022 The condition of masking quantum qutric ststes *Laser Phys. Lett.* **19** 115201
[21] Li B *et al* 2019 Deterministic versus probabilistic quantum information masking *Phys. Rev.* A **99** 052343
[22] Lie S H and Jeong H 2020 Randomness cost of masking quantum information and the information conservation law *Phys. Rev.* A **101** 052322
[23] Liu Z H *et al* 2021 Photonic implementation of quantum information masking *Phys. Rev. Lett.* **126** 170505
[24] Du Y *et al* 2021 Masking quantum information encoded in pure and mixed states *Int. J. Theor. Phys.* **60** 2380–99
[25] Li M S and Modi K 2020 Probabilistic and approximate masking of quantum information *Phys. Rev.* A **102** 022418
[26] Zhu H J 2021 Hiding and masking quantum information in complex and real quantum mechanics *Phys. Rev. Res.* **3** 033176
[27] Shi F, Li M S, Chen L and Zhang X 2021 *k*-uniform quantum information masking *Phys. Rev.* A **104** 032601
[28] Zhang S M, Wang M H and Zhou B 2023 Quantifying the information distribution of quantum information masking *Quantum Inf. Process.* **22** 284
[29] Shang W M, Fan X Y, Zhang F L and Chen J L 2023 Quantum information masking of an arbitrary unknown state can be realized in the multipartite lower-dimensional systems *Phys. Scr.* **98** 035102

[30] Shen Y, Zhang F L, Chen Y Z and Zhou C C 2023 Masking quantum information in the Kitaev Abelian anyons *Phys.* A **612** 128495
[31] Wang M Y *et al* 2024 Masking quantum information in multipartite systems based on generator matrices *Laser Phys.* **34** 055203
[32] Shen Y *et al* 2024 Anyonic quantum multipartite maskers in the Kitaev model *Phys. Rev.* A **109** 032421
[33] Arnaud L and Cerf N J 2013 Exploring pure quantum states with maximally mixed reductions *Phys. Rev.* A **87** 012319
[34] Goyeneche D and Zyczkowski K 2014 Genuinely multipartite entangled states and orthogonal arrays *Phys. Rev.* A **90** 022316
[35] Rao C R 1946 Hypercubes of strength'd'leading to confounded designs in factorial experiments *Bull. Calcutta Math. Soc.* **38** 67–78
[36] Hedayat A S, Sloane N J A and Stufken J 2012 *Orthogonal Arrays: Theory and Applications* (Springer)
[37] Cheng C S 1980 Orthogonal arrays with variable numbers of symbols *Ann. Stat.* **8** 447–53