Max-Planck-Institut für Mathematik in den Naturwissenschaften Leipzig

Quantum Information Masking of Hardmard Sets

by

Bao-Zhi Sun, Shao-Ming Fei, and Xianqing Li-Jost

Preprint no.: 32 2020

Quantum Information Masking of Hardmard Sets

Bao-Zhi Sun

*School of Mathematical Sciences, Qufu Normal University, Shandong 273165, China**

Shao-Ming Fei

School of Mathematical Sciences, Capital Normal University, Beijing 100048, China and Max-Planck-Institute for Mathematics in the Sciences, Leipzig 04103, Germany†

Xianqing Li-Jost

Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany‡

Abstract

We study quantum information masking of arbitrary dimensional states. We present the condition that the linear combination of fixed reducing states has the same marginal states as the fixed reducing ones. We define so called Hardmard set of quantum states whose Gram-Schmidt matrix can be diagonalized by Hardmard unitary matrices. We show that any Hardmard set can be deterministically masked by a unitary operation. Accounting to that a linear combination of fixed reducing states may have the same marginal states as the fixed reducing ones, we analyze the states which can be masked together with the given Hardmard set. Detailed examples are given to illustrate our results.

PACS numbers: 03.67.-a, 32.80.Qk

*Electronic address: wenyuesbz@qq.com

†Electronic address: feishm@cnu.edu.cn

‡Electronic address: xianqing.li-jost@mis.mpg.de

I. INTRODUCTION

Due to the linearity of quantum evolution, there are many distinguished features in quantum physics such as non-cloning [1–3], non-broadcasting [4] and non-deleting [5]. These phenomena are closely related to quantum information processing like key distribution [6, 7], quantum teleportation [8, 9] and communication security protocols [10, 11]. They are also connected to the conversation of information and the second law of thermodynamics [12, 13].

Recently, Kavan Modi et. al. investigated the problem of quantum information masking [14]. They obtained the so-called no-masking theorem, saying that it is impossible to mask all arbitrary pure states by the same unitary operator. The masking schemes in multipartite scenario [15, 16], probabilistic quantum information masking [17], and a complete characterization of qubit masking [18], and probabilistic and approximate masking of quantum information based on completely positive and trace decreasing (invertible) linear transformations [19] have been presented.

Quantum information masking has potential applications in secret sharing [20–22]. A maskable set may have uncountably many elements that are not orthogonal to each other. The main problem in quantum information masking is to ascertain which set of quantum states can be masked. In this paper, we study the quantum masking of arbitrary dimensional systems based on unitary operations and Hardmard matrices.

II. QUANTUM INFORMATION MASKING AND HARDMARD SETS

We denote $\mathcal{H}_X$ the $d-$dimensional Hilbert space associated with the system X. A unitary operator $\mathcal{U}$ masks the quantum information contained in a set of states $\{|a_k\rangle_A \in \mathcal{H}_A\}_{k=1}^n$, if it maps $|a_k\rangle_A$ to $|\Psi_k\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B,\ k = 1, 2, \cdots, n$ such that all the reduced states of $|\Psi_k\rangle_{AB}$ are identical,

$$\mathrm{Tr}_B|\Psi_k\rangle_{AB}\langle\Psi_k| = \rho_A, \quad \mathrm{Tr}_A|\Psi_k\rangle_{AB}\langle\Psi_k| = \rho_B,\ \forall k = 1, 2, \cdots, n. \tag{1}$$

The reduced states ρ_A and ρ_B contain no information about the value of k. The set $\{|a_k\rangle_A\}_{k=1}^n$ is said to be maskable with respect to the masker $\mathcal{U}$.

A set of bipartite pure states $\{|\Psi_k\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B\}_{k=1}^n$ is called a set of fixed reducing states if they have identical marginal states, namely, the relations (1) are satisfied. Given a

bipartite pure state $|\Psi_0\rangle_{AB}$, with Schmidt decomposition:

$$|\Psi_0\rangle_{AB} = \sum_{j=1}^{r} \lambda_j |\phi_j\rangle_A \otimes |\psi_j\rangle_B.$$

$\sum_j \lambda_j^2 |\phi_j\rangle_A\langle\phi_j|$ and $\sum_j \lambda_j^2 |\psi_j\rangle_B\langle\psi_j|$ are the spectral decompositions of $\rho_A = \mathrm{Tr}_B|\Psi\rangle_{AB}\langle\Psi|$ and $\rho_B = \mathrm{Tr}_A|\Psi\rangle_{AB}\langle\Psi|$, respectively. Conversely, if $\rho_A = \sum_j \lambda_j^2 |\xi_j\rangle\langle\xi_j|$ and $\rho_B = \sum_j \lambda_j^2 |\varsigma_j\rangle\langle\varsigma_j|$ are the spectral decompositions of ρ_A and ρ_B, respectively, the following pure bipartite state

$$|\Psi\rangle = \sum_j \lambda_j |\xi_j\rangle \otimes |\varsigma_j\rangle$$

has the same reducing states as $|\Psi_0\rangle_{AB}$. If the Schmidt coefficients of $|\Psi_0\rangle_{AB}$ are all not equal, then $|\phi_j\rangle$ and $|\xi_j\rangle$ ($|\psi_j\rangle$ and $|\varsigma_j\rangle$) only differ by a phase.

It has been shown in [17] that a set of fixed reducing states $\{|\Psi_k\rangle_{AB}\}_{k=1}^n$ can always be written in the following form:

$$|\Psi_k\rangle_{AB} = \sum_{j=1}^{r} \lambda_j |\phi_j\rangle_A \otimes |\psi_j^{(k)}\rangle_B, \quad k = 1, 2, \cdots, n, \tag{2}$$

where $\{\lambda_j\}_{j=1}^r$ are nonzero Schmidt coefficients of $|\Psi_k\rangle$, r is their Schmidt rank. $\rho_A = \sum_j \lambda_j^2 |\phi_j\rangle_A\langle\phi_j|$ ($\rho_B = \rho_B^{(k)} = \sum_j \lambda_j^2 |\psi_j^{(k)}\rangle_B\langle\psi_j^{(k)}|$) is a certain spectral decomposition of ρ_A (ρ_B), $k = 1, 2, \cdots, n$.

We first consider that, for a given set of n fixed reducing states $\{|\Psi_k\rangle_{AB}\}_{k=1}^n$, how to add a new state to $\{|\Psi_k\rangle_{AB}\}_{k=1}^n$ so as to get a set of $n+1$ fixed reducing states. Denote

$$\begin{aligned} |\Psi(\vec{\mu})\rangle &= \sum_k \mu_k |\Psi_k\rangle_{AB} = \sum_k \mu_k \sum_j \lambda_j |\phi_j\rangle \otimes |\psi_j^{(k)}\rangle \\ &= \sum_j \lambda_j |\phi_j\rangle \otimes (\sum_k \mu_k |\psi_j^{(k)}\rangle) = \sum_j \lambda_j |\phi_j\rangle \otimes |\psi_j(\vec{\mu})\rangle, \end{aligned} \tag{3}$$

where

$$|\psi_j(\vec{\mu})\rangle = \sum_k \mu_k |\psi_j^{(k)}\rangle, \quad j = 1, 2, \ldots, r. \tag{4}$$

$|\psi_j(\vec{\mu})\rangle$ is some linear combination of the eigenvectors of ρ_B corresponding to eigenvalue λ_j. The problem is to find the conditions for $\vec{\mu}$ such that $|\Psi(\vec{\mu})\rangle$ has the same reduced density matrices as $\{|\Psi_k\rangle\}$.

Theorem 1. *Let $\{|\Psi_k\rangle\}_{k=1}^n$ and $|\Psi(\vec{\mu})\rangle$ be the states given in (2) and (3), respectively. Then $\{|\Psi_k\rangle\}_{k=1}^n \cup \{|\Psi(\vec{\mu})\rangle\}$ constitute a set of fixed reducing states if and only if*

$$\delta_{jj'} = \langle\psi_{j'}(\vec{\mu})|\psi_j(\vec{\mu})\rangle = \sum_{k,k'} \mu_k \mu_{k'}^* \langle\psi_{j'}^{(k')}|\psi_j^{(k)}\rangle, \quad j, j' = 1, 2, \cdots, r. \tag{5}$$

Proof: Without loss of generality, assume that

$$\omega_1 = \lambda_1 = \cdots = \lambda_{j_1} \neq \omega_2 = \lambda_{j_1+1} = \cdots = \lambda_{j_2} \neq \omega_3 \cdots \neq \omega_m = \lambda_{j_{m-1}+1} = \cdots = \lambda_r.$$

Then, for any $|\Psi(\vec{\mu})\rangle$ given in (3) we have

$$\rho_B(\vec{\mu}) = \mathrm{Tr}_A |\Psi(\vec{\mu})\rangle\langle\Psi(\vec{\mu})| = \sum_{i=1}^{m} \omega_i P_i(\vec{\mu}). \tag{6}$$

For $|\Psi_k\rangle$ given in (2), the reduced states have the form,

$$\rho_B = \mathrm{Tr}_A |\Psi_k\rangle\langle\Psi_k| = \sum_{i=1}^{m} \omega_i P_i, \tag{7}$$

where $P_i = \sum_{j=j_{i-1}+1}^{j_i} |\psi_j\rangle\langle\psi_j|$ is the orthogonal projector onto the eigensubspace $\mathcal{H}_i$ corresponding to ω_i, and $P_i(\vec{\mu}) = \sum_{j=j_{i-1}+1}^{j_i} |\psi_j(\vec{\mu})\rangle\langle\psi_j(\vec{\mu})|$ is an projector onto the same subspace as P_i.

From the basic acknowledge of algebra, $\rho_B = \rho_B(\vec{\mu})$ if and only if $P_i = P_i(\vec{\mu})$ for $i = 1, 2, \cdots, m$. Furthermore, $\{|\psi_j\rangle\}_{j=j_{i-1}+1}^{j_i}$ is an orthonormal bases for $\mathcal{H}_i$. Denote

$$\Psi_i = \Big(\, |\psi_{j_{i-1}+1}\rangle \ \cdots \ |\psi_{j_i}\rangle \, \Big)$$

and

$$\Psi_i(\vec{\mu}) = \Big(\, |\psi_{j_{i-1}+1}(\vec{\mu})\rangle \ \cdots \ |\psi_{j_i}(\vec{\mu})\rangle \, \Big).$$

Then $P_i = \Psi\Psi^\dagger$, $P_i(\vec{\mu}) = \Psi(\vec{\mu})\Psi^\dagger(\vec{\mu})$. We have

$$\begin{aligned} I &= \Psi^\dagger\Psi = \Psi^\dagger\Psi\Psi^\dagger\Psi = \Psi^\dagger\Psi(\vec{\mu})\Psi^\dagger(\vec{\mu})\Psi \\ &= \Psi^\dagger(\vec{\mu})\Psi\Psi^\dagger\Psi(\vec{\mu}) = \Psi^\dagger(\vec{\mu})\Psi(\vec{\mu})\Psi^\dagger(\vec{\mu})\Psi(\vec{\mu}) \\ &= \big(\Psi^\dagger(\vec{\mu})\Psi(\vec{\mu})\big)^2, \end{aligned}$$

where the fourth equality is due to that $\Psi^\dagger\Psi(\vec{\mu})$ is a square matrix. Hence, $\big(\Psi^\dagger\Psi(\vec{\mu})\big)^{-1} = \Psi^\dagger(\vec{\mu})\Psi$. Since $\Psi^\dagger(\vec{\mu})\Psi(\vec{\mu})$ is positive, we have $\Psi^\dagger(\vec{\mu})\Psi(\vec{\mu}) = I$. Therefore, we obtain that $\{|\psi_j(\vec{\mu})\rangle\}_{j=j_{i-1}+1}^{j_i}$ is also an orthonormal bases for $\mathcal{H}_i$, i.e., $\delta_{jj'} = \langle\psi_{j'}(\vec{\mu})|\psi_j(\vec{\mu})\rangle$ for $j, j' = j_{i-1}+1, \cdots, j_i$. Noting that the eigenvectors corresponding different eigenvalues are always orthogonal, we conclude that "only if" part of the theorem is true.

Now suppose $\delta_{jj'} = \langle\psi_{j'}(\vec{\mu})|\psi_j(\vec{\mu})\rangle$ for $j, j' = 1, 2, \cdots, r$. Then certainly $\rho_A(\vec{\mu}) = \rho_A$. Because $\{|\psi_j\rangle\}_{j=j_{i-1}+1}^{j_i}$ and $\{|\psi_j(\vec{\mu})\rangle\}_{j=j_{i-1}+1}^{j_i}$ are two orthonormal bases for $\mathcal{H}_i$, it is easy to prove that $P_i = P_i(\vec{\mu})$, $i = 1, 2, \cdots, m$. Then we have $\rho_B(\vec{\mu}) = \rho_B$, which completes the proof. ■

As applications, let us consider the following two cases:

i). $\{\lambda_j\}_{j=1}^r$ are all different. In this case, with respect to the eigenvalue λ_j, the eigenvectors $|\psi_j^{(k)}\rangle$ and $|\psi_j^{(k')}\rangle$ differ only by a phase. Assume

$$|\Psi_k\rangle = \sum_{j=1}^{r} \lambda_j |\phi_j\rangle \otimes e^{i\theta_{jk}} |\psi_j\rangle, \quad k = 1, 2, \cdots, n, \tag{8}$$

then $|\Psi(\vec{\mu})\rangle = \sum_j \lambda_j |\phi_j\rangle \otimes (\sum_k \mu_k e^{i\theta_{jk}})|\psi_j\rangle$ and $|\psi_j(\vec{\mu})\rangle = (\sum_k \mu_k e^{i\theta_{jk}})|\psi_j\rangle$. One has $\langle\psi_{j'}^{(k')}|\psi_j^{(k)}\rangle = 0$ for different j, j' and arbitrary k, k'. The condition (5) becomes $|\sum_k \mu_k e^{i\theta_{jk}}| = 1$, $j = 1, 2, \cdots, n$.

ii). $\{\lambda_j\}_{j=1}^r$ are all equal. In this case $\{|\psi_j^{(k)}\rangle\}_{j=1}^r$ can be any orthonormal bases in the support of ρ_B in $\mathcal{H}_B$. $|\Psi_k\rangle$ can be written as,

$$|\Psi_k\rangle = \frac{1}{\sqrt{r}} \sum_{j=1}^{r} |\phi_j\rangle \otimes |\psi_j^{(k)}\rangle, \quad k = 1, 2, \cdots, n \tag{9}$$

One has $|\Psi(\vec{\mu})\rangle = \frac{1}{\sqrt{r}} \sum_j |\phi_j\rangle \otimes (\sum_k \mu_k |\psi_j^{(k)}\rangle)$ and $|\psi_j(\vec{\mu})\rangle = \sum_k \mu_k |\psi_j^{(k)}\rangle$. The condition that $|\Psi(\vec{\mu})\rangle$ has the same marginal states as $|\Psi_k\rangle$ is equivalent to that $\langle\psi_{j'}(\vec{\mu})|\psi_j(\vec{\mu})\rangle = \delta_{j'j}$, $\forall j', j$, i.e., $\vec{\mu}^\dagger A_{j'j} \vec{\mu} = \delta_{j'j}$, where $A_{j'j} = (\langle\psi_{j'}^{(k')}|\psi_j^{(k)}\rangle)_{k',k}$.

We now consider the quantum masking of a special set of Hardmard states. We call a unitary matrix $U = (u_{jk}) \in \mathcal{C}^{n\times n}$ a Hardmard one if all the entries u_{jk} have the same modular $\frac{1}{\sqrt{n}}$, i.e., $u_{jk} = \frac{1}{\sqrt{n}} e^{i\theta_{jk}}$.

Give a set of states $\{|a_k\rangle_A \in \mathcal{H}_A\}_{k=1}^n$, the so-called Gram-Schmidt matrix of the set is given by $G = (\langle a_k|a_l\rangle)_{n\times n}$. It is well known that Gram-Schmidt matrix of a set of states is a positive Hermitian matrix. It can be diagonalized by unitary transformations. We consider special sets of states $\{|a_k\rangle_A \in \mathcal{H}_A\}_{k=1}^n$. We call $\{|a_k\rangle_A \in \mathcal{H}_A\}_{k=1}^n$ a Hardmard set if the corresponding Gram-Schmidt matrix can be diagonalized by Hardmard unitary matrix, i.e., there exits a Hardmard unitary matrix U, such that

$$G = (\langle a_k|a_l\rangle) = U^\dagger \mathrm{diag}(\lambda_1, \lambda_2, \cdots, \lambda_n) U. \tag{10}$$

Obviously, any orthonormal basis of a quantum system is a Hardmard set because the related Gram-Schmidt matrix is the unit matrix.

Theorem 2. *A Hardmard set $\{|a_k\rangle_A \in \mathcal{H}_A\}_{k=1}^n$, $n \leq d$, can be deterministically masked by a unitary operation.*

Proof: Suppose $G = (\langle a_k|a_{k'}\rangle) = U^\dagger \mathrm{diag}(\lambda_1^2, \lambda_2^2, \cdots, \lambda_n^2)U$, $U = \frac{1}{\sqrt{n}}(e^{i\theta_{jk}})$. Let $\{|\phi_j^A\rangle\}_{j=1}^n$ and $\{|\psi_j^B\rangle\}_{j=1}^n$ be arbitrary orthonormal sets in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Set

$$|\Psi_k\rangle = \frac{1}{\sqrt{n}} \sum_{j=1}^{n} \lambda_j e^{i\theta_{jk}} |\phi_j^A\rangle \otimes |\psi_j^B\rangle, \quad k = 1, 2, \cdots, n. \tag{11}$$

Then

$$\mathrm{Tr}_A |\Psi_k\rangle\langle\Psi_k| = \frac{1}{n} \sum_{j=1}^{n} \lambda_j^2 |\psi_j^B\rangle\langle\psi_j^B| = \rho_B, \tag{12}$$

$$\mathrm{Tr}_B |\Psi_k\rangle\langle\Psi_k| = \frac{1}{n} \sum_{j=1}^{n} \lambda_j^2 |\phi_j^A\rangle\langle\phi_j^A| = \rho_A. \tag{13}$$

This means that $\{|\Psi_k\rangle\}$ is a fixed reducing set. Furthermore, we have:

$$\langle\Psi_k|\Psi_{k'}\rangle = \frac{1}{n} \sum_j \lambda_j^2 e^{i\theta_{jk'}} e^{-i\theta_{jk}} = \left(U^\dagger \mathrm{diag}(\lambda_1^2, \lambda_2^2, \cdots, \lambda_n^2)U\right)_{kk'}.$$

Hence

$$(\langle\Psi_k|\Psi_{k'}\rangle) = U^\dagger \mathrm{diag}(\lambda_1^2, \lambda_2^2, \cdots, \lambda_n^2)U = (\langle a_k|a_{k'}\rangle).$$

Let $|\phi_0\rangle \in \mathcal{H}_B$. Denote $|\tilde{a}_k\rangle = |a_k\rangle \otimes |\phi_0\rangle$, $k = 1, 2, \cdots, n$. Then $(\langle\Psi_k|\Psi_{k'}\rangle) = (\langle\tilde{a}_k|\tilde{a}_{k'}\rangle)$. Since two sets of states $\{|\tilde{a}_k\rangle\}_{k=1}^n$ and $\{|\Psi_k\rangle\}_{k=1}^n$ have the same Gram-Schmidt matrices, there exists a unitary operator V such that $V|\tilde{a}_k\rangle = |\Psi_k\rangle$ for $k = 1, 2, \cdots, n$. Namely, the Hardmard set $\{|a_k\rangle_A \in \mathcal{H}_A\}_{k=1}^n$, $n \leq d$, can be deterministically masked. ■

We have shown that a Hardmard set $\{|a_k\rangle\}_{k=1}^n$ can be deterministically masked by a unitary operation. Consider $|a(\vec{\mu})\rangle = \sum_k \mu_k |a_k\rangle$. Then V changes $|a(\vec{\mu})\rangle$ to

$$|\Psi(\vec{\mu})\rangle = \sum_k \mu_k |\Psi_k\rangle = \frac{1}{\sqrt{n}} \sum_j \lambda_j |\phi_j^A\rangle \otimes (\sum_k \mu_k e^{i\theta_{jk}}) |\psi_j^B\rangle. \tag{14}$$

From Theorem 1, V can mask the set of states $\{|a_k\rangle\}_{k=1}^n$ and $|a(\vec{\mu})\rangle$ together if and only if

$$\delta_{jj'} = \langle\psi_{j'}(\vec{\mu})|\psi_j(\vec{\mu})\rangle, j, j' = 1, 2, \cdots, n, \tag{15}$$

where $|\psi_j(\vec{\mu})\rangle = \frac{1}{\sqrt{n}}(\sum_k \mu_k e^{i\theta_{jk}})|\psi_j^B\rangle$. Because $\langle\psi_j^B|\psi_{j'}^B\rangle = \delta_{jj'}$, (15) is equivalent to $\frac{1}{n}|(\sum_k \mu_k e^{i\theta_{jk}})|^2 = 1$. From the above analysis, we have the following result.

Theorem 3. *Suppose $\{|a_k\rangle_A \in \mathcal{H}_A\}_{k=1}^n$ is a Hardmard set such that its Gram-Schmidt matrix is diagonalized by Hardmard unitary matrix U. Then $|a(\vec{\mu})\rangle = \sum_k \mu_k |a_k\rangle$ and $\{|a_k\rangle\}_{k=1}^n$ together can be masked by some masker V if and only if $|(U\vec{\mu})_j| = 1$, $j = 1, 2, \cdots, n$, where $\vec{\mu} = (\mu_1, \mu_2, \cdots, \mu_n)^t$.*

We now present some examples to illustrate our results.

Example 1. Suppose that $\{|a_k\rangle\}_{k=1}^d$ is just an orthonormal bases of $\mathcal{H}_A$. For any Harmard matrix $U = \frac{1}{\sqrt{d}}(e^{i\theta_{jk}})$, and orthonormal bases $\{|\phi_k\rangle_A\}_{k=1}^d$, $\{|\psi_k\rangle_B\}_{k=1}^d$ in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, the fixed reducing states can be chosen to be

$$|\Psi_k\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_j e^{i\theta_{jk}} |\phi_j\rangle_A \otimes |\psi_j\rangle_B, \quad k = 1, 2, \cdots, d.$$

The masker which transforms $|a_k\rangle \otimes |0\rangle_B$ to $|\Psi_k\rangle_{AB}$, $k = 1, 2, \cdots, d$, can be constructed in the following way. We expand $\{|a_k\rangle \otimes |0\rangle_B\}_{k=1}^d$ and $\{|\Psi_k\rangle_{AB}\}_{k=1}^d$ to two orthonormal bases of $\mathcal{H}_A \otimes \mathcal{H}_B$ as $\{|a_k\rangle \otimes |l-1\rangle_B\}_{k,l=1}^d$ and $\{|\Psi_k\rangle_{AB}\}_{k=1}^d \cup \{|\phi_k\rangle_A \otimes |\psi_l\rangle_B\}_{k\neq l=1}^d$, respectively. Then using $\{|a_k\rangle \otimes |l-1\rangle_B\}_{k,l=1}^d$ as columns, we obtain a unitary matrix $\mathcal{U}_1$ with the first n columns given by $\{|a_k\rangle \otimes |0\rangle\}_{k=1}^d$. Similarly, we have $\mathcal{U}_2$ with the first d columns given by $|\Psi_k\rangle_{AB}$, $k = 1, 2, \cdots, d$, and the other columns given by $\{|\phi_k\rangle_A \otimes |\psi_l\rangle_B\}_{k\neq l=1}^d$. Then $\mathcal{U}_2\mathcal{U}_1^\dagger$ is the masker which transforms $|a_k\rangle \otimes |0\rangle_B$ to $|\Psi_k\rangle_{AB}$ for $k = 1, 2, \cdots, d$.

Example 2. Consider the qubit case $d = 2$. Given an arbitrary linear independent set $\{|a_1\rangle, |a_2\rangle\}$, the GS-matrix can be written as

$$G = \begin{pmatrix} 1 & re^{-i\theta} \\ re^{i\theta} & 1 \end{pmatrix}.$$

The two eigenvalues of G are equal if and only if $r = 0$. If $r = 0$, the unitary matrix to diagonalize G can be selected arbitrary. If $r \neq 0$, simple calculation gives rise to that the elements of the eigenvectors of G have the same modulus. Then $|a_1\rangle, |a_2\rangle$ is a Hardmard set. All the related Hardmard matrices can be written as:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\omega_1} & e^{i\omega_2} \\ e^{i(\omega_1+\theta)} & -e^{i(\omega_2+\theta)} \end{pmatrix} \equiv U(\omega_1, \omega_2), \quad \forall \omega_1, \omega_2.$$

that is, $U^\dagger(\omega_1, \omega_2)\, G\, U(\omega_1, \omega_2) = \begin{pmatrix} 1+r & 0 \\ 0 & 1-r \end{pmatrix}$. Then the corresponding fixed reducing set is of the form,

$$|\Psi_1\rangle = \tfrac{1}{\sqrt{2}}[e^{i\omega_1}|\phi_1\rangle \otimes |\psi_1\rangle + e^{i(\omega_1+\theta)}|\phi_2\rangle \otimes |\psi_2\rangle],$$
$$|\Psi_2\rangle = \tfrac{1}{\sqrt{2}}[e^{i\omega_2}|\phi_1\rangle \otimes |\psi_1\rangle - e^{i(\omega_2+\theta)}|\phi_2\rangle \otimes |\psi_2\rangle].$$

Set $V_1 = (|a_1\rangle \otimes |0\rangle\, |a_2\rangle \otimes |0\rangle) U(\omega_1, \omega_2) \begin{pmatrix} \frac{1}{\sqrt{1+r}} & 0 \\ 0 & \frac{1}{\sqrt{1-r}} \end{pmatrix}$. We have $V_1^\dagger V_1 = I_2$. Expanding

V_1 to an unitary matrix $V = (V_1\ V_2)$ on $\mathcal{H}_2 \otimes \mathcal{H}_2$, we get

$$V^\dagger(|a_1\rangle \otimes |0\rangle\ |a_2\rangle \otimes |0\rangle)U(\omega_1,\omega_2)\begin{pmatrix} \frac{1}{\sqrt{1+r}} & 0 \\ 0 & \frac{1}{\sqrt{1-r}} \end{pmatrix} = \begin{pmatrix} \sqrt{1+r} & 0 \\ 0 & \sqrt{1-r} \\ 0 & 0 \\ 0 & 0 \end{pmatrix}. \tag{16}$$

Similarly, set $W_1 = (|\Psi_1\rangle\ |\Psi_2\rangle)U(\omega_1,\omega_2)\begin{pmatrix} \frac{1}{\sqrt{1+r}} & 0 \\ 0 & \frac{1}{\sqrt{1-r}} \end{pmatrix}$. We get another unitary matrix $W = (W_1\ W_2)$,

$$W^\dagger(|\Psi_1\rangle\ |\Psi_2\rangle)U(\omega_1,\omega_2)\begin{pmatrix} \frac{1}{\sqrt{1+r}} & 0 \\ 0 & \frac{1}{\sqrt{1-r}} \end{pmatrix} = \begin{pmatrix} \sqrt{1+r} & 0 \\ 0 & \sqrt{1-r} \\ 0 & 0 \\ 0 & 0 \end{pmatrix}. \tag{17}$$

From (16) and (17), we have

$$V^\dagger(|a_1\rangle \otimes |0\rangle\ |a_2\rangle \otimes |0\rangle) = W^\dagger(|\Psi_1\rangle\ |\Psi_2\rangle).$$

Therefore,

$$WV^\dagger(|a_1\rangle \otimes |0\rangle\ |a_2\rangle \otimes |0\rangle) = (|\Psi_1\rangle\ |\Psi_2\rangle).$$

Then, $WV^\dagger$ is a corresponding masker.

Furthermore, any qubit pure state can be expressed as $|a(u_1,u_2)\rangle = u_1|a_1\rangle + u_2|a_2\rangle$. From Theorem 3, we have that the states $|a_1\rangle, |a_2\rangle, |a(u_1,u_2)\rangle$ can be masked if and only if there exists some ω_i, $i = 1,2$, such that $U(\omega_1,\omega_2)\begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$ has unimodular elements. This is certainly true for every $|a(u_1,u_2)\rangle$. Therefore, we can conclude that for qubit systems, any three states can be masked by a unitary masker, which is accordance with the results in [18].

III. CONCLUSION

The so-called no-go theories are of great significance in information processing like key distribution and quantum teleportation. No-masking theory is a new no-go theory introduced by Modi *et al.* [23]. We have studied the masking problem based on Hardmard

matrices. We have derived the condition that the linear combination of fixed reducing states has the same marginal states as the fixed reducing ones. We have shown that any set of quantum states whose Gram-Schmidt matrix can be diagonalized by Hardmard unitary matrices can be deterministically masked by a unitary operation. The states which can be masked together with a given Hardmard set have been also investigated. Our approach may highlight further researches on quantum information masking.

Acknowledgments This work is supported by the NSF of China under grant Nos. 11675113, 11701320, Shandong provincial NSF of China grant No. ZR2016AM04, Beijing Municipal Commission of Education under grant No. KZ201810028042, and Beijing Natural Science Foundation (Z190005).

---

[1] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned.* Nature (London) **299**, 802 (1982).

[2] N. Gisin and S. Massar, *Optimal Quantum Cloning Machines.* Phys. Rev. Lett. **79**, 2153 (1997).

[3] A. Lamas-Linares, C. Simon, J. C. Howell, and D. Bouwmeester, *Experimental Quantum Cloning of Single Photons.* Science **296**, 712 (2002).

[4] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, *Noncommuting Mixed States Cannot Be Broadcast.* Phys. Rev. Lett. **76**, 2818 (1996).

[5] A. K. Pati and S. L. Braunstein, *Impossibility of deleting an unknown quantum state.* Nature (London) **404**, 164 (2000).

[6] Won-Young Hwang, *Quantum Key Distribution with High Loss: Toward Global Secure Communication.* Phys. Rev. Lett. **91**, 057901 (2003)

[7] V. Scarani, H. B-Pasquinucci, Nicolas J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution.* Rev. Mod. Phys. **81**, 1301 (2009)

[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels.* Phys. Rev. Lett. **70**, 1895 (1993).

[9] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, *Experimental quantum teleportation.* Nature (London) **390**, 575-579(1997).

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography.* Rev. Mod. Phys. **74**, 145 (2002).

[11] Samuel L. Braunstein, and Peter van Loock, *Quantum information with continuous variables.* Rev. Mod. Phys. **77**, 513 (2005)

[12] M. Horodecki, R. Horodecki, A. Sen(De), and U. Sen, *No-deleting and no-cloning principles as consequences of conservation of quantum information.* arXiv: quant-ph/0306044.

[13] M. Horodecki, R. Horodecki, A. Sen(De), and U. Sen, *Common origin of no-cloning and no-deleting principles - Conservation of information.* Found. Phys. **35**, 2041 (2005).

[14] K. Modi, A. K. Pati, A. Sen(De), *Masking Quantum Information is Impossible.* Phys. Rev. Lett. **120**, 230501 (2018).

[15] J. I. de Vicente, C. Spee, and B. Kraus, *Maximally Entangled Set of Multipartite Quantum States.* Phys. Rev. Lett. **111**, 110502(2013)

[16] M. Sh. Li, and Y. L. Wang, *Masking quantum information in multipartite scenario.* Phys. Rev. A **98**, 062306 (2018)

[17] B. Li, S. h. Jiang, X. B. Liang, X. Li-Jost, H. Fan, and S. M. Fei, *Deterministic versus probabilistic quantum information masking.* Phys. Rev. A **99**, 052343 (2019)

[18] X. B. Liang, B. Li, and S. M. Fei, *Complete characterization of qubit masking.* Phys. Rev. A **100**, 030304(R) (2019)

[19] M. S. Li, K. Modi, *Probabilistic and Approximate Masking of Quantum Information.* arXiv:1912.02419.

[20] M. Hillery, V. Bužek, and A. Berthiaume, *Quantum secret sharing.* Phys. Rev. A **59**, 1829 (1999).

[21] R. Cleve, D. Gottesman, and H. K. Lo, *How to Share a Quantum Secret.* Phys. Rev. Lett. **83**, 648 (1999).

[22] H. Lu, Zh. Zhang, L. K. Chen, Zh-D Li, Ch. L., Li Li, N-L Liu, X. F. Ma, Y. A. Chen, and J-W Pan, *Secret Sharing of a Quantum State.* Phys. Rev. Lett. **117**, 030501 (2016).

[23] K. Modi, A. K. Pati, A. Sen(De), and U. Sen, *Masking Quantum Information is Impossible.* Phys. Rev. Lett. **120**, 230501 (2018).