Journal of Quantum Computing
DOI:10.32604/jqc.2020.015855
Article

The Development and Application of Quantum Masking

Tao Chen[1,2], Zhiguo Qu[1,2,*] and Yi Chen[1,2]

[1]School of Computer & Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[2]Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[*]Corresponding Author: Zhiguo Qu. Email: qzghhh@126.com
Received: 15 November 2020; Accepted: 20 December 2020

Abstract: To solve the problem of hiding quantum information in simplified subsystems, Modi et al. [1] introduced the concept of quantum masking. Quantum masking is the encoding of quantum information by composite quantum states in such a way that the quantum information is hidden to the subsystem and spreads to the correlation of the composite systems. The concept of quantum masking was developed along with a new quantum impossibility theorem, the quantum no-masking theorem. The question of whether a quantum state can be masked has been studied by many people from the perspective of the types of quantum states, the number of masking participants, and error correction codes. Others have studied the relationships between maskable quantum states, the deterministic and probabilistic masking of quantum states, and the problem of probabilistic masking. Quantum masking techniques have been shown to outperform previous strategies in quantum bit commitment, quantum multi-party secret sharing, and so on.

Keywords: Quantum masking; quantum systems; maximal maskable set

1 Introduction

It has always been an important and meaningful task to explore the demarcation criterion between quantum and classical information. Entanglement, as a unique property of quantum, plays a very important role in distinguishing quantum information from classical information. Due to the existence of entanglement, quantum information exhibits some powers that far exceed classical information, such as quantum invisible transfer states, ultra-dense coding, etc. A series of quantum unknowns are derived from this. A series of quantum impossibility theorems, such as the quantum no-cloning [2,3] theorem, the quantum no-deletion [4] theorem, etc., are derived from the linearity and unity of quantum mechanics.

While the storage of classical information depends on the system, quantum information can be hidden in the correlation of two systems. Recently Modi et al. [1] have investigated whether quantum information can only be stored in the quantum correlation of two quantum systems, rather than in the systems themselves. Their quantum state encoding process is known as masking, which makes the pre-masking information inaccessible to both quantum systems. Based on the linearity and unity of quantum mechanics, Modi et al. also highlight an impossibility theorem, the quantum non-masking theorem. The theorem is that it is impossible to mask any one quantum state in a two-party quantum system.

Of course, quantum masking is more than that; it still leaves many questions to be answered. For example, how do you determine the maskable range of a given quantum masking operator? What happens if the quantum information is masked in a mixed state system, rather than a pure state system? For a

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

quantum state, when is it deterministic masking and when is it probabilistic masking? Is it possible to derive its maskable probability? In terms of masking methods, it has been proposed in the literature [5] that masking of quantum information into multiple quantum states is feasible using quantum error correction codes, but do other methods exist? Cao et al. [6] also investigated how to find the maximum maskable set for a masking operator, which gives a conclusion to the conjecture 5 proposed by Modi et al. in paper [1]. Cao et al. also introduced maskable of a set of mixed states by extending the case of pure states, and showed that there is also no-masking theorem in mixed states. Li et al. [7] studied what kind of quantum states can be masked deterministically or probabilistically, and proved that a set of mutually orthogonal quantum states can be masked deterministically, while a set of linearly independent quantum states can be masked probabilistically. Liang et al. [8] systematically studied the masking problem of quantum information systems, complete depiction of the maskable set through several theorems, and gave that the largest maskable set on a Bloch sphere is the set of states of a spherical circle, and that all states of an arbitrary sphere on a Bloch sphere are maskable.

2 Quantum Masking

We first give the basic concept of quantum masking and its definition, as well as the basic content of the quantum no-masking theorem.

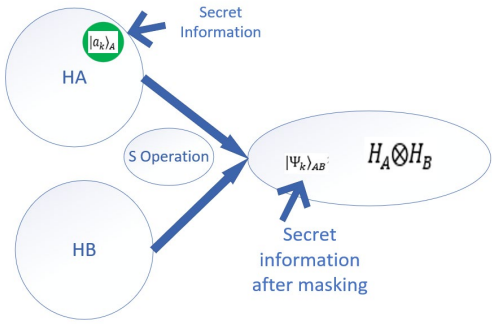

Figure 1: Combining the secret information of the system HA with the auxiliary particles of the system HB and masking the original secret information into a composite system after the masking operator S operation

Definition 1: An existing unitary operation S is called a masking operator, which serves to map a quantum state to be masked $\{ |a_k\rangle_A \in H_A \}$ into a composite system $\{ |\Psi_k\rangle_{AB} \in H_A \otimes H_B \}$ and for which all marginal measurements are the same for the mapped quantum state, i.e.,

$$\rho_A = Tr_B(|\Psi_k\rangle_{AB}\langle\Psi_k|) \quad \text{and} \quad \rho_B = Tr_A(|\Psi_k\rangle_{AB}\langle\Psi_k|) \tag{1}$$

That is, we cannot learn any information about $|a_k\rangle_A$ from $|\Psi_k\rangle_{AB}$. This way we can mask the quantum information that we want to mask to a set of correlations of a composite system.

This S we also call a masker. The process can be described as a physical process, so the operation can be implemented by introducing an auxiliary particle, described as:

$$S: U_S|a_k\rangle_A \otimes |b\rangle_B = |\Psi_k\rangle_{AB} \ , \ |b\rangle_B \in H_B \tag{2}$$

Since the masking operator S is a linear transformation, it does not change the orthogonality of the basis, and in addition to this, if S can mask a set of basis states $\{ |a_k\rangle_A\}$, then S can mask the quantum information contained in its density matrix $\{ |a_k\rangle\langle a_k|\}$.

Theorem 1: No masker can mask all states of a qubit in H^2.

A detailed proof of Theorem 1 can be found in literature [1]. This theorem is identical to the quantum non-cloning theorem and the quantum non-deletion theorem; in fact, the set of maskable states in the quantum non-maskable theorem is much richer than the set of no-cloning and no-deleting states.

3 Exploration of Quantum Masking

We go on to give some of the exploration of quantum masking by a number of existing researchers.

3.1 Masking Quantum Information in Multipartite Scenario

Li et al. [5] study how to mask quantum information in multiparty systems and successfully extend it to arbitrary higher-order quantum systems. First, a simple particle is given as an example to illustrate how to mask a quantum state into a multi-particle quantum system.

Lemma 1: Here a quantum state $|\Psi\rangle$ is a quantum state in multi-partite system $\bigotimes_{j=1}^{n} H_{A_j}$. For any $|\Psi_j\rangle$, $\{j=1, 2, \ldots, n\}$ can be written as: $\sum_{k=1}^{n_j} c_k|\psi_k\rangle_{A_j}|\mu_k\rangle_{\widehat{A_j}}$. Here $\widehat{A_j}=(\bigotimes_{j=1}^{n} H_{A_j}) / A_j$, and $|\psi_k\rangle$, $|\mu_k\rangle$ are all orthogonal bases, And we can have the following results for the partial trace:

$$\rho_{A_j}= Tr_{\widehat{A_j}}(|\Psi\rangle\langle\Psi|)= \sum_{k=1}^{n_j} |c_k|^2 |\psi_k\rangle_{A_j}\langle\psi_k| \tag{3}$$

Proof.

$$\begin{aligned}
&\rho_{A_j}= Tr_{\widehat{A_j}}(|\Psi\rangle\langle\Psi|) \qquad (4)\\
&= Tr_{\widehat{A_j}}(\sum_{k=1}^{n_j}\sum_{l=1}^{n_j} c_k\bar{c_l} |\psi_k\rangle_{A_j}\langle\psi_l| \otimes|\mu_k\rangle_{\widehat{A_j}}\langle\mu_l|)\\
&= \sum_{k=1}^{n_j}\sum_{l=1}^{n_j} c_k\bar{c_l} |\psi_k\rangle_{A_j}\langle\psi_l| * Tr(|\mu_k\rangle_{\widehat{A_j}}\langle\mu_l|)\\
&= \sum_{k=1}^{n_j}\sum_{l=1} c_k\bar{c_l} |\psi_k\rangle_{A_j}\langle\psi_l| *\delta_{kl}\\
&= \sum_{k=1}^{n_j} |c_k|^2 |\psi_k\rangle_{A_j}\langle\psi_k|
\end{aligned}$$

Example 1:

The masking process for all quantum states can be defined as follows:

$$\begin{aligned}
|0\rangle=|\psi_0\rangle&= \frac{|00\rangle+|11\rangle}{\sqrt{2}}\otimes\frac{|00\rangle+|11\rangle}{\sqrt{2}}\\
|1\rangle=|\psi_1\rangle&= \frac{|00\rangle-|11\rangle}{\sqrt{2}}\otimes\frac{|00\rangle-|11\rangle}{\sqrt{2}}
\end{aligned} \tag{5}$$

$Proof.$ Existence a quantum states$|\alpha\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, then after quantum masking operation it can be changed into $|\psi\rangle = \alpha_0|\psi_0\rangle + \alpha_1|\psi_1\rangle$. After substitution using Lemma 1, the quantum state $|\psi\rangle$ can be reduced to:

$$\frac{\alpha_0+\alpha_1}{2}(|0000\rangle+|1111\rangle)+\frac{\alpha_0-\alpha_1}{2}(|0011\rangle+|1100\rangle) \tag{6}$$

Due to these quantum state $|000\rangle, |111\rangle, |011\rangle, |100\rangle$ are all orthogonal. So we calculate using Appendix's Lemma 1 to get:

$$\begin{aligned}
&\rho_A = Tr_A(|\psi\rangle\langle\psi|)\\
&= \frac{1}{2}(|0\rangle\langle 0|+|1\rangle\langle 1|)
\end{aligned}$$

$$= \frac{I}{2} \tag{7}$$

Therefore, based on the symmetry of the four systems, we can conclude that for any j all can get $\rho_A = \frac{I}{2}$.

So, According to Example1, we extend it to get:

Theorem 2: For any integer $d \geq 2$, then we can mask all the quantum states in C^d just by adding $2d-1$ systems which have the same dimension. That is, they can be masked in the multi-partite system $\bigotimes_{j=1}^{d} H_j$, $H_j = C^d$. Here we give a simple proof.

Proof. Let $|0\rangle, |1\rangle, \ldots, |d\text{-}1\rangle$ be an orthogonal normalized basis of C^d. Now we can define the unitary processing as:

$$|l\rangle \rightarrow |\varphi_l\rangle = \bigotimes_{j=1}^{d} \frac{\sum_{k=0}^{d-1} \omega^{kl} |kk\rangle}{\sqrt{d}}, \quad l \in \{0,1,2,\ldots,d\text{-}1\} , \quad \omega = e^{\frac{2\pi i}{d}} \tag{8}$$

For an arbitrary quantum state $|\alpha\rangle = \sum_0^{d-1} \alpha_l |l\rangle$, It will be transformed by the masking operator into $|\varphi_\alpha\rangle = \sum_0^{d-1} \alpha_l |\varphi_l\rangle$. In a similar way to Example1, we finally solve for its partial trace to obtain:

$\rho_{A_1} = Tr_{\widehat{A_1}}(|\varphi_\alpha\rangle\langle\varphi_\alpha|)$

$$= \frac{d^{d-1}}{d^{d-1}} \left(\sum_{j=0}^{d-1} \left| \frac{\sum_{k=0}^{d-1} \omega^{jk} \alpha_k}{\sqrt{d}} \right|^2 \right) \left(\sum_{l=0}^{d-1} |l\rangle\langle l| \right) \tag{9}$$

$$= \frac{1}{d} I_d$$

The reader is referred to Document [5] for a detailed proof of the procedure.

The authors also study the problem of masking of quantum states in tripartite subsystems. Unlike the approach using error-correcting codes, the authors use a pair of mutually orthogonal Latin squares. Three matrices are considered in order to represent the masking process of the target in the tripartite systems. The authors first give two orthogonal Latin squares of dimension d and show how the masking process can be constructed using these two Latin squares.

Theorem 3: Let d be an integer and greater than 2, this is, $d \geq 3$ and $d \in N$. If there exist $V, W \in M_d(C)$ such that they are orthogonal Latin squares labeled by symbols $\{1, 2, \ldots, d\}$, then all the d level quantum states can be masked by the process changed into tripartite systems $C^d \otimes C^d \otimes C^d$.

3.2 Masking Quantum Information Encoded in Pure a Mixed States

Cao et al. studied the maskable of quantum masks in the pure state and mixed state with sufficient necessary conditions, and proposed methods for solving the maximum maskable set in the pure state and mixed state, respectively.

Cao found four states which cannot be masked. Let $|\psi_1\rangle, |\psi_2\rangle \in S_A$ with $\langle\psi_1|\psi_2\rangle = 0$. Then

$$Q = \left\{ |\psi_1\rangle, |\psi_2\rangle, \frac{1}{\sqrt{2}}(|\psi_1\rangle + |\psi_2\rangle), \frac{1}{\sqrt{2}}(|\psi_1\rangle - i|\psi_2\rangle) \right\} \tag{10}$$

The four states cannot be masked by a linear operator S: $H_A \rightarrow H_A \otimes H_B$.

4 Applications of Quantum Masking

We give an overview of the existing and possible applications of quantum masking. Quantum masking techniques have been shown to work well in quantum bit commitments.

4.1 No Qubit Commitment

In a bit commitment protocol, Alice and Bob are on both sides of the correspondence. First, Alice commits to a bit 0 or 1 and later she provides Bob classical or quantum information that reveals the committed bit. In fact, an ideal quantum bit committed protocol should ensure Bob that Alice is indeed committed to her initial bit and Bob can learn no information about the committed bit before the opening phase. However, the entanglement based cheating strategy makes any quantum bit commitment protocol impossible in the nonrelativistic domain. Let us briefly recall the cheating strategy. Suppose that Alice prepares two two-particle quantum states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ corresponding to bit 0 or 1, keeps one particle, and sends the other to Bob. As Bob has no information about 0 or 1, this makes the reduced density matrix $\rho_B = \mathrm{Tr}_A|\Psi_0\rangle\langle\Psi_0| = \mathrm{Tr}_A|\Psi_1\rangle\langle\Psi_1|$. This condition then implies that $|\Psi_0\rangle = \sum_i \sqrt{\lambda_i}\,|a_i^0\rangle|b_i\rangle$ and $|\Psi_1\rangle = \sum_i \sqrt{\lambda_i}\,|a_i^1\rangle|b_i\rangle$. However, $|\Psi_0\rangle = U_A \otimes I_B|\Psi_1\rangle$ as they differ only by a local change of basis. This is the key to cheating, because during the unveiling stage, Alice can decide to do nothing or apply a local unitary on her particle. Thus, she can always cheat on her committed bit. An analysis of the performance of quantum bit commitment based on quantum masking can be found in [1].

Quantum masking can be applied not only to quantum bit commitments, but also to quantum multi-party secret sharing, quantum information steganography, and other areas.

5 Conclusion

After analysis, we can find that quantum masking, as a new technique also based on quantum entanglement properties, has made a major contribution to further clarify the demarcation line between quantum information and classical information, and has successfully explored the quantum no-masking theorem. We also analyze the explorations of some scholars on quantum masking, which are very valuable. Finally, we analyze the possible applications of quantum masking, all of which have good prospects and are worthy of further exploration.

Acknowledgement: This work was supported by the innovation and entrepreneurship training program of Nanjing University of Information Science & Technology (No. 202010300212). I want to thank my teacher for his encouragement and help all the time, and I will go forward unswervingly.

Funding Statement: This work was supported by the innovation and entrepreneurship training program of Nanjing University of Information Science & Technology (No. 202010300212). Grantee: Chen. Sponsors' websites: http://sjjx.nuist.edu.cn:81/CXCY/.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

Reference

[1] K. Modi, A. K. Pati, A. Sen and U. Sen, "Masking quantum information is impossible," *Physical Review Letters,* vol. 120, no. 1, pp. 34–39, 2018.

[2] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 1, pp. 802–803, 1982.

[3] D. Martini, F. Bužek and V. Sciarrino, "Experimental realization of the quantum universal NOT gate," *Nature,* vol. 419, no. 1, pp. 815–818, 2002.

[4] A. K. Pati. and S. L. Braunstein, "Impossibility of deleting an unknown quantum state," *Nature*, vol. 404, no.1, pp. 164–165, 2000.

[5] M.S. Li and Y. L. Wang, "Masking quantum information in multipartite scenario", *Physical Review A,* vol. 98, no. 1, pp. 42–47, 2018.

[6] H. X. Cao, "Masking quantum information encoded in pure and mixed states" *International Journal of Theoretical Physics*, 2020. [Online]. Available: https://doi.org/10.1007/s10773-020-04542-w.

[7] B. Li, S. H. Jiang, X. B. Liang, X. Q. Li, Fan and H. Fei, "Quantum information masking: Deterministic versus probabilistic," *Physical Review A,* vol. 99, no. 1, pp. 23–28, 2019.

[8] X. B. Liang, B. Li and S. M. Fei, "Complete characterization of qubit masking," *Physical Review A,* vol. 100, no. 1, pp. 30–34, 2019.