


# Blind quantum computation with a client performing different single-qubit gates

Guang-Yang Wu(吴光阳), Zhen Yang(杨振), Yu-Zhan Yan(严玉瞻),Yuan-Mao Luo(罗元茂), Ming-Qiang Bai(柏明强), and Zhi-Wen Mo(莫智文)

**Citation:**Chin. Phys. B, 2023, 32 (**11**): 110302. DOI: 10.1088/1674-1056/ace15a

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

**What follows is a list of articles you may be interested in**

---

## Variational quantum semi-supervised classifier based on label propagation

Yan-Yan Hou(侯艳艳), Jian Li(李剑), Xiu-Bo Chen(陈秀波), and Chong-Qiang Ye(叶崇强)

Chin. Phys. B, 2023, 32 (**7**): 070309. DOI: 10.1088/1674-1056/acb9fb

## Circuit quantum electrodynamics with a quadruple quantum dot

Ting Lin(林霆), Hai-Ou Li(李海欧), Gang Cao(曹刚), and Guo-Ping Guo(郭国平)

Chin. Phys. B, 2023, 32 (**7**): 070307. DOI: 10.1088/1674-1056/accd57

## Energy shift and subharmonics induced by nonlinearity in a quantum dot system

Yuan Zhou(周圆), Gang Cao(曹刚), Hai-Ou Li(李海欧), and Guo-Ping Guo(郭国平)

Chin. Phys. B, 2023, 32 (**6**): 060303. DOI: 10.1088/1674-1056/acc521

## Nonadiabatic geometric phase in a doubly driven two-level system

Weixin Liu(刘伟新), Tao Wang(汪涛), and Weidong Li(李卫东)

Chin. Phys. B, 2023, 32 (**5**): 050311. DOI: 10.1088/1674-1056/ac89e3

## Analysis and improvement of verifiable blind quantum computation

Min Xiao(肖敏) and Yannan Zhang(张艳南)

Chin. Phys. B, 2022, 31 (**5**): 050305. DOI: 10.1088/1674-1056/ac2f34

---

# Blind quantum computation with a client performing different single-qubit gates

Guang-Yang Wu(吴光阳)[1,2,3], Zhen Yang(杨振)[1,2,3], Yu-Zhan Yan(严玉瞻)[1,2,3], Yuan-Mao Luo(罗元茂)[1,2,3], Ming-Qiang Bai(柏明强)[1,2,3,†], and Zhi-Wen Mo(莫智文)[1,2,3]

[1] *School of Mathematical Sciences, Sichuan Normal University, Chengdu* 610068, *China*
[2] *Research Center of Sichuan Normal University National-Local Joint Engineering Laboratory of System Credibility Automatic Verification, Chengdu* 610066, *China*
[3] *Institute of Intelligent Information and Quantum Information, Sichuan Normal University, Chengdu* 610068, *China*

(Received 4 April 2023; revised manuscript received 8 June 2023; accepted manuscript online 25 June 2023)

In the field of single-server blind quantum computation (BQC), a major focus is to make the client as classical as possible. To achieve this goal, we propose two single-server BQC protocols to achieve verifiable universal quantum computation. In these two protocols, the client only needs to perform either the gate $T$ (in the first protocol) or the gates $H$ and $X$ (in the second protocol). With assistance from a single server, the client can utilize his quantum capabilities to generate some single-qubit states while keeping the actual state of these qubits confidential from others. By using these single-qubit states, the verifiable universal quantum computation can be achieved.

**Keywords:** blind quantum computation, verifiable blind quantum computation, single server

**PACS:** 03.67.Lx, 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/ace15a

## 1. Introduction

As is well known, quantum computation has significant advantages over classical computation in solving some problems.[1,2] This means that quantum computation may become essential for many people in the future. However, Feynman[3] pointed out that it is impossible to represent the results of quantum mechanics with a classical universal device, this may prompt some people to explore how to build quantum computers. Actually, when the first generation of quantum computers comes out, they may be accessible to a few people around the world. In other words, many people cannot access to use quantum computers directly. Thus, when someone wants to use a quantum computer to achieve computation, he may delegate his quantum computation to the owner of the quantum computer. Unfortunately, some private information may be leaked out in this process. To solve this problem, researchers proposed the idea of blind quantum computation (BQC).

Childs[4] firstly proposed the BQC protocol in 2005. In that protocol, the client needs to prepare quantum states, store quantum states, and perform the SWAP gate. Since then, many BQC protocols have been proposed one by one.[5–13] For example, Broadbent *et al.*[12] proposed the first universal blind quantum computation (UBQC) protocol. Compared with Ref. [4], that protocol further limits the quantum ability of the client. In the protocol, the client only needs to prepare single-qubit states. Based on the fact that measuring single-qubit states is easier than preparing single-qubit states in experimental setups, Morimae and Fujii[13] proposed a new type of BQC protocol in 2013, where the client needs to measure single-qubit states rather than to prepare single-qubit states. Moreover, some BQC protocols have been experimentally demonstrated.[14,15]

To make the client completely classical in the BQC protocol, some scholars have made in-depth research. For example, Broadbent *et al.* extended the UBQC protocol to a double-server protocol in Ref. [12], in which the client is completely classical. After this, Li *et al.*[16] proposed a triple-server BQC protocol. Then, Xu *et al.*[17] modified this protocol to a single-server BQC protocol. They both declared that the client is completely classical in their respective protocols. However, Hung and Hwang[18] pointed out a security loophole in those two protocols. Even more unfortunately, Morimae *et al.*[19] declared that the client cannot be completely classical in the single-server BQC protocol. Thus, making the client as classical as possible becomes a hot research in single-server BQC protocol.

It is worth noting that verifiability is an important property in the BQC protocol. This means that the client can make sure the result of delegate quantum computation to be correct or incorrect. In order to achieve this goal, some verifiable BQC protocols are proposed. In 2015, Hayashi and Morimae[20] proposed a protocol based on the fact that graph states can be completely specified by a set of stabilizer operators. In 2017, Fitzsimons and Kashefi[21] proposed the unconditional verifiable blind quantum computation (VUBQC) protocol according to the way of the UBQC protocol. In those two protocols, the client can verify the correctness of the delegated quantum

†Corresponding author. E-mail: baimq@sicnu.edu.cn
© 2023 Chinese Physical Society and IOP Publishing Ltd

computation according to whether the server is honest or dishonest.

In 2021, Li *et al.*[22] proposed a new type of BQC protocol, where the client only needs to perform a few single-qubit gates. Specifically, the client needs to perform the gates $H, T$ or the gates $T, X$. As we all know, the gates $H, T$ can be used to fit any single-qubit gates. In order to further limit the quantum ability of the client, we propose two single-server BQC protocols in this paper. The first protocol allows the client to perform the gate $T$. In the second protocol, the client is allowed to perform the gates $T, X$. In addition, the client does not have any quantum abilities in these two protocols. Although we weaken the quantum ability of the client, our protocol can still achieve verifiable blind quantum computation.

The rest of this paper is organized as follows. In order to better understand the proposed protocols, we first review a related protocol in Section 2. Section 3 will be divided into two subsections to propose our two protocols. Section 4 analyzes the proposed protocols from two aspects, i.e., correctness and safety. Finally, we provide conclusions in Section 5.

## 2. Preliminaries

In this section, we review the VUBQC protocol, which plays an important role in the proposed protocols. In this protocol, the client only needs to prepare some single-qubit states. Specifically, the client can prepare the state of the qubits that is one of the set $\{|0\rangle, |1\rangle, |\theta\rangle\}$, $\theta \in \{\frac{k\pi}{4}, k = 0, 1, \ldots, 7\}$. The VUBQC protocol can be described as follows:

(A1) Alice converts her input $x$ and quantum computation $\mathcal{C}$ into a pair $(G, \{\phi_i\})$, where $G$ is a universal graph state and $\{\phi_i\}$ is the associated set of computational angles.

(A2) Alice prepares $M+T+D$ single-qubit states, where $M$ qubits will be used for computation, $T$ qubits will be used as trap qubits, the state of these qubits is one of the set $|\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$, $\theta \in \{\frac{k\pi}{4}, k = 0, 1, \ldots, 7\}$; $D$ qubits will be used as dummy qubits, the state of these qubits is $|0\rangle$ or $|1\rangle$.

(A3) Alice sends all single-qubit states to Bob. Then Bob performs the gate $CZ$ to entangle them according to the graph state $G$, where an embedding of $T$ trap qubits and $D$ dummy qubits can be admited.

(A4) Alice asks Bob to measure the following qubits: (1) If the qubit is a computation qubit, it will be measured in the basis $\{|\pm\delta\rangle\}$, where $\delta = \phi' + \theta + r\pi$, $\theta$ is the angle of the qubit in (A2), $\phi'$ is a modification of $\phi$ according to previous measurement results, $\phi$ is the actual measurement angel, $r$ is encryption to the result. (2) If the qubit is a trap qubit, Bob can use the basis $\{|\pm(\theta + r\pi)\rangle\}$ to measure it. Similarly, $\theta$ is the angle of the qubit in (A2), $r$ is encryption to the result. (3) If the qubit is a dummy qubit, it will be measured in the basis $\{\pm\theta\}$, $\theta \in \{\frac{k\pi}{4}, k = 0, 1, \ldots, 7\}$. After Bob measures the qubit, he sends the measurement result to Alice.

(A5) After all qubits were measured, Alice will check the results of trap qubits. If all results of trap qubits are correct, then Alice can think that Bob does not perform any malicious operations. Finally, Alice undoes the impact of $r$ to recover the correct outcome of this delegated quantum computation; otherwise the protocol will be stopped.

## 3. Main protocol

### 3.1. Blind quantum computation with a client only performing the gate $T$

In this subsection, the client Alice only performs the gate $T$. Suppose that Alice wants to achieve the same goal like the VUBQC protocol. Now, she wants to finish her computation on the $N$-qubit graph state corresponding to the graph $G$, where $N = M+T+D$. The graph $G$ admits an embedding of $D$ dummy qubits and $T$ trap qubits. The process of this protocol is shown in Fig. 1.

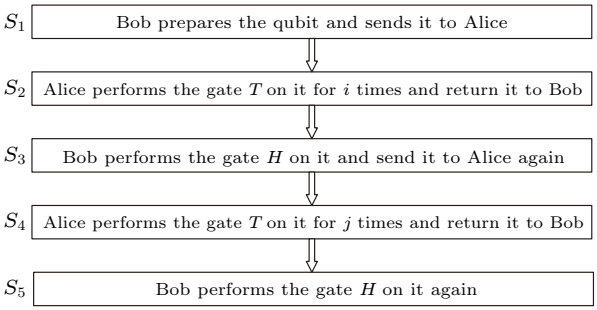



**Fig. 1.** Blind quantum computation with a client only performing the gate $T$.

The specific steps are given as follows:

(T1) Alice asks Bob to prepare $M+T+D+S$ qubits in state $|+\rangle$. These qubits will be divided into three sets, the set $P_1$ is made up of $M+T$ qubits, in which $M$ qubits for computation and $T$ qubits as trap qubits; $D$ qubits as dummy qubits make up the set $P_2$; the rest of $S$ qubits as decoy qubits make up the set $P_3$.

(T2) Bob sends a qubit to Alice, then Alice performs one of the following operations: (i) If the qubit is from the set $P_1$, Alice will perform the gate $T$ on it for $n$ times in order to make the state of the qubit be $|\theta\rangle$, $\theta \in \{\frac{n\pi}{4}, n = 0, 1, \ldots, 7\}$. (ii) If the qubit is from the set $P_2$, Alice will perform the gate $T$ on it for 2 or 6 times, then the state of the qubit will be $|\frac{\pi}{2}\rangle$ or $|\frac{3\pi}{2}\rangle$. (iii) If the qubit is from the set $P_3$, Alice will perform the corresponding single-qubit gate to make the state of the qubit be one of $\{|+\rangle, |-\rangle, |\frac{\pi}{2}\rangle, |\frac{3\pi}{2}\rangle\}$, where $|+\rangle = |+\rangle$, $|-\rangle = T^4|+\rangle$, $|\frac{\pi}{2}\rangle = T^2|+\rangle$, $|\frac{3\pi}{2}\rangle = T^6|+\rangle$.

(T3) Alice asks Bob to perform the gate $H$ once on all qubits.

(T4) Bob sends a qubit to Alice, then Alice performs one of the following operations: (i) If the qubit is from the set $P_1$, Alice will do nothing. (ii) If the qubit is from the set $P_2$, Alice

will perform the gate $T$ on it for 2 times or 6 times in order to make the state of the qubit be $|+\rangle$ or $|-\rangle$. (iii) If the qubit is from the set $P_3$, Alice will perform the gate $T$ on it for 2 times in order to make the state of the qubit be one of the set $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$. Finally, Alice returns the qubit to Bob.

(T5) Alice reveals which qubits belong to the set $P_3$, then she asks Bob to measure these $S$ decoy qubits in the basis $\{|+\rangle,|-\rangle\}$ or $\{|0\rangle,|1\rangle\}$. After Bob measured these decoy qubits, Alice and Bob will compare the results. If Bob can always publish the correct result when he chooses the right basis, Alice and Bob can make sure that there is no attack; otherwise the protocol aborts.

(T6) Alice asks Bob to perform the gate $H$ once on all qubits again.

(T7) Alice and Bob use these qubits to perform the VUBQC protocol.

When steps (T1)–(T6) are successfully performed, the states of these qubits will be $HT^jHT^i|+\rangle$. We should note that there are some certain constraints on the values of $i$ and $j$. Specifically, if $j=0$, the value of $i$ belongs to the set $\{0,1,\ldots,7\}$; if $j=2$, the value of $i$ only can be 2 or 6. Obviously, according to the value of $i$ and $j$, the states of the qubits belong to the set $\{|0\rangle,|1\rangle,|\theta\rangle\}$, $\theta\in\{\frac{k\pi}{4},k=0,1,\ldots,7\}$. For example, if $i=3$, $j=0$, the qubit will be in state $|\frac{3\pi}{4}\rangle$; if $i=2$, $j=2$, the qubit will be in state $|0\rangle$.

### 3.2. Blind quantum computation with a client performing the gates *T, X*

In this subsection, the client Alice can perform the gates $T,X$. Actually, based on the fact that $HXH=Z$, the client can also perform the gate $Z$. Now, suppose that Alice wants to achieve the same goal like the VUBQC protocol and finish her computation on the $N$-qubit graph state corresponding to the graph $G$. Figure 2 shows the process of the protocol, in which the values of $i,j,k$ will be 0 or 1.

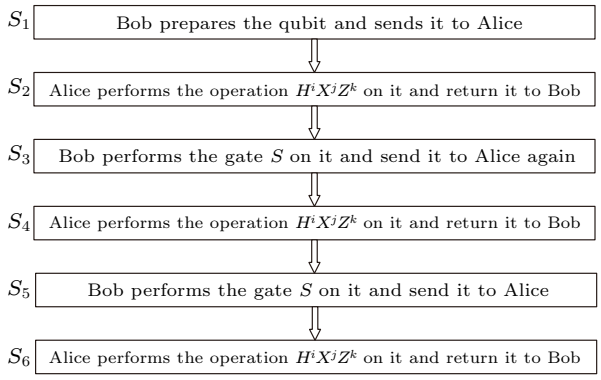



**Fig. 2.** Blind quantum computation with a client performing the gates $T,X$.

The specific steps are given as follows:

(S1) Alice asks Bob to prepare $M+T+D+S$ qubits in state $|0\rangle$, where $M=M_1+M_2+M_3$, $T=T_1+T_2+T_3$. These qubits will be divided into five sets, the set $W_i$ is made up of $M_i+T_i$ qubits, in which $M_i$ qubits for computation and $T_i$ qubits as trap qubits, $i=1,2,3$; $D$ qubits as dummy qubits make up the set $W_4$; the rest of $S$ qubits as decoy qubits make up the set $W_5$.

(S2) Bob sends a qubit to Alice, then Alice performs one of the following operations: (i) If the qubit is from the set $W_1$, Alice will perform the corresponding single-qubit gate to make the state of the qubit be $|+\rangle$ or $|-\rangle$, where $|+\rangle=H|0\rangle=XH|0\rangle$, $|-\rangle=HX|0\rangle=HXHXH|0\rangle$. (ii) If the qubit is from the set $W_5$, Alice will perform the corresponding single-qubit gate to make the state of the qubit be $|0\rangle$ or $|1\rangle$, where $|0\rangle=|0\rangle=HXH|0\rangle$, $|1\rangle=X|0\rangle=XHXH|0\rangle$. (iii) If the qubit is from other sets, Alice will do nothing. Finally, Alice returns the qubit to Bob.

(S3) Alice asks Bob to perform the gate $T$ once on all qubits.

(S4) Bob sends a qubit to Alice, then Alice performs one of the following operation: (i) If the qubit is from the set $W_1$, Alice will perform the corresponding single-qubit gate to make the state of the qubit be $|\frac{k\pi}{4}\rangle$, $k=1,3,5,7$, where $|\frac{\pi}{4}\rangle=|\frac{\pi}{4}\rangle=HXH|\frac{5\pi}{4}\rangle$, $|\frac{3\pi}{4}\rangle=HXHX|\frac{\pi}{4}\rangle=X|\frac{5\pi}{4}\rangle$, $|\frac{5\pi}{4}\rangle=HXH|\frac{\pi}{4}\rangle=|\frac{5\pi}{4}\rangle$, $|\frac{7\pi}{4}\rangle=X|\frac{\pi}{4}\rangle=HXHX|\frac{5\pi}{4}\rangle$. (ii) If the qubit is from the set $W_2$, Alice will perform the corresponding single-qubit gate to make the state of the qubit be $|+\rangle$ or $|-\rangle$. (iii) If the qubit is from other sets, Alice will do nothing. Finally, Alice returns the qubit to Bob.

(S5) Alice asks Bob to perform the gate $S$ once on all qubits.

(S6) Bob sends a qubit to Alice, then Alice performs one of the following operation: (i) If the qubit is from the set $W_1$ or $W_2$, Alice will do nothing. (ii) If the qubit is from the set $W_3$, Alice will perform the corresponding single-qubit gate to make the state of the qubit be $|+\rangle$ or $|-\rangle$. (iii) If the qubit is from the set $W_4$, Alice will perform the corresponding single-qubit gate to make the state of the qubit be $|0\rangle$ or $|1\rangle$. (iv) If the qubit is from the set $W_5$, Alice will perform the corresponding single-qubit gate to make the state of the qubit be one of $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$. Finally, Alice returns the qubit to Bob.

(S7) Alice reveals which qubits belong to the set $W_5$, then Bob measures these $S$ decoy qubits on the bases $\{|0\rangle,|1\rangle\}$ or $\{|+\rangle,|-\rangle\}$. After Bob measured these decoy qubits, Alice and Bob will compare the results. If Bob can always publish the correct result when he chooses the right basis, Alice and Bob can make sure that there is no attack; otherwise the protocol aborts.

(S8) Alice and Bob use these qubits to perform the VUBQC protocol.

When steps (S1)–(S7) are successfully performed, the qubits from different sets will be different states. For example, the qubits from the set $W_1$ will be in state $|\frac{k\pi}{4}\rangle$, $k=1,3,5,7$;

the qubits from the set $W_4$ will be in state $|0\rangle$ or $|1\rangle$. Actually, the state of these qubits will belong to the set $\{|0\rangle, |1\rangle, |\theta\rangle\}$, $\theta \in \{\frac{k\pi}{4}, k = 0, 1, \ldots, 7\}$.

## 4. Analysis

Obviously, if there is an outside attacker in these two protocols, she or he will be discovered with a high probability when Alice asks Bob to measure the decoy qubits. Thus, the outside attacker will be ignored when complaining the correctness of these two protocols.

**Theorem 1** Assume that Bob follows the step of these two protocols, then the outcome is correct.

**Proof** In the first protocol, when Alice and Bob perform the corresponding operations, the qubits will be in state $HT^jHT^i|+\rangle$. Firstly, when $j = 0$, then the state of the qubit will be $|\frac{i\pi}{4}\rangle$, $i = 0, 1, \ldots, 7$. Secondly, if $j = 2$, $i = 6$ or 2, the qubit will be in state $|0\rangle$ or $|1\rangle$. Thus, Alice can generate ten types of single-qubit states, which is one of the set $\{|0\rangle, |1\rangle, |\frac{\theta}{4}\rangle\}$, $\theta \in \{\frac{k\pi}{4}, k = 0, 1, \ldots, 7\}$. Using these qubits, the VUBQC protocol can be realized. As we all know, when the VUBQC protocol is successfully performed, the outcome is correct.

In the second protocol, it can also generate the resource states when Alice and Bob perform the corresponding operations. Firstly, if the qubit is from the set $W_1$, the state of the qubit will be $|\frac{k\pi}{4}\rangle$, $k = 1, 3, 5, 7$. Secondly, if the qubit is from the set $W_2$, the state of the qubit will be $|\frac{\pi}{2}\rangle$ or $|\frac{3\pi}{2}\rangle$. Thirdly, if the qubit is from the set $W_3$, the state of the qubit will be $|+\rangle$ or $|-\rangle$. Fourthly, if the qubit is from the set $W_4$, the state of the qubit will be $|0\rangle$ or $|1\rangle$. Thus, Alice can generate the resource state when she can perform the gates $T, X$ with the help of Bob. Finally, Alice and Bob use these qubits to achieve the VUBQC protocol. Similarly, the outcome is correct when the VUBQC protocol is successfully performed.

**Theorem 2** In these two protocols, Bob cannot learn any useful information about the actual input, output and algorithm.

**Proof** In the first protocol, the state of the qubit will be $HT^jHT^i|+\rangle$ when Alice and Bob perform the corresponding operations. In the whole process, Bob does not know how many times Alice performed the gate $T$ on the qubit. Based on this fact, Bob does not know the actual values of $i$ and $j$. This is the reason why he cannot get any information about the actual state of the qubit. Thus, Bob cannot learn any useful information about the actual input, output and algorithm when they use these qubits to perform the VUBQC protocol.

In the second protocol, Alice will perform three quantum operations in the whole process. These operations will be recorded $U_1$, $U_2$, and $U_3$. Firstly, when Alice performs the operation $U_1$ on the qubits, the states of the qubits belong to the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Secondly, when Alice performs the operation $U_2$ on the qubits, the states of the qubits belong to the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |\frac{\pi}{4}\rangle, |\frac{3\pi}{4}\rangle, |\frac{5\pi}{4}\rangle, |\frac{7\pi}{4}\rangle\}$. Thirdly, when Alice performs the operation $U_3$ on the qubits, the states of the qubits belong to the set $\{|0\rangle, |1\rangle, |\frac{\theta}{4}\rangle\}$, $\theta \in \{\frac{k\pi}{4}, k = 0, 1, \ldots, 7\}$. Obviously, when Alice performs the quantum operations on all qubits, the states of these qubits are not orthogonal. This is the reason why Bob cannot distinguish these qubits from each other. Thus, Bob cannot learn any useful information about the actual input, output and algorithm when they use these qubits to perform the VUBQC protocol.

## 5. Conclusions

In the single-server BQC protocol, there are main three models according to the quantum ability of the client. The first model is proposed by Broadbent *et al.*,[12] it allows the client to prepare the single-qubit states. Morimae and Fujii[13] proposed the second model, where the client needs to measure the single-qubit states. The third model is proposed by Li *et al.*,[22] it allows the client to perform the single-qubit gates. Obviously, the first two protocols proposed are based on the third model. Compared to Ref. [22], the proposed protocols further limit the quantum ability of the client. Specifically, the first protocol allows the client to perform the gate $T$ rather than the gates $H, T$; the second protocol allows the client to perform the gates $T, X$ instead of the gates $H, T$.

The proposed protocols require bidirectional transmission of quantum states between client and server. As we all know, quantum states will encounter some unavoidable problems in the process of transmission. For example, they will be affected by noise when they are transmitted in the channel. Compared with one-way transmission of quantum states, bidirectional transmission of quantum states is more affected by noise. Up to date, there are some BOC protocols[23–26] that can resist the effects of noise. These protocols mainly use entanglement distillation and error-correcting codes to resist noise, both of which require some quantum power. If these two methods are simply added to the proposed protocol, it may be contrary to the original intention of the proposed protocol. When the client only can perform a few single-qubit gates, what methods should be taken to resist the noise? This is a question worth thinking about.

## Acknowledgments

Project supported by the National Science Foundation of Sichuan Province (Grant No. 2022NSFSC0534), the Central Guidance on Local Science and Technology Development Fund of Sichuan Province (Grant No. 22ZYZYTS0064), the Chengdu Key Research and Development Support Program (Grant No. 2021-YF09-0016-GX), and the Key Project of Sichuan Normal University (Grant No. XKZX-02).

## References


[1] Grover L K 1997 *Phys. Rev. Lett.* **79** 325
[2] Shor P W 1994 *Proceedings 14th Annual Symposium on Foundations of Computer Science*, November 20–22, 1994, Santa Fe, NM, USA, p. 124
[3] Richard P F 1982 *Int. J. Theor. Phys.* **21** 467
[4] Childs A M 2005 *Quantum Inf. Comput.* **5** 456
[5] Dorit A, Michael B, Elad E and Urmila M 2017 arXiv:1704.04487 [quant-ph]
[6] Dunjko V, Kashefi E and Leverrier A 2012 *Phys. Rev. Lett.* **108** 200502
[7] Morimae T 2012 *Phys. Rev. Lett.* **109** 230502
[8] Mantri A, Pérez-Delgado C A and Fitzsimons J F 2013 *Phys. Rev. Lett.* **111(23)** 230502
[9] Carlos A P and Joseph F F 2015 *Phys. Rev. Lett.* **114** 220502
[10] Giovannetti V, Maccone L, Morimae T and Rudolph T G 2013 *Phys. Rev. Lett.* **111** 230501
[11] Arrighi P and Salvail L 2006 *Int. J. Quantum Inf.* **4** 05
[12] Broadbent A, Fitzsimons J and Kashefi E 2009 *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, October 25–27, 2009, Atlanta, GA, USA, p. 517
[13] Morimae T and Fujii K 2013 *Phys. Rev. A* **87** 050301
[14] Barz S, Kashefi E, Broadbent A, Barz S, Kashefi E, Broadbent A, Fitzsimons J, Zeilinger A and Walther P 2012 *Science* **335** 308
[15] Greganti C, Roehsner C M, Barz S, Morimae T and Walther P 2016 *New J. Phys.* **18** 013020
[16] Li Q, Chan W H, Wu C H and Wen Z H 2014 *Phys. Rev. A* **89** 040302
[17] Xu H R and Wang B H 2021 *Laser Phys. Lett.* **19**015202
[18] Hung S M and Hwang T 2015 arXiv:1508.07478 [quant-ph]
[19] Morimae T, Nishimura H, Takeuchi Y and Tani S 2018 arXiv:1812.03703v1 [quant-ph]
[20] Hayashi M and Morimae T 2015 *Phys. Rev. Lett* **115** 220502
[21] Fitzsimons J F and Kashefi E 2017 *Phys. Rev. A* **96** 012303
[22] Li Q, Liu C D, Peng Y, Yu F and Zhang C 2021 *Opt. Laser Technol.* **142** 107190
[23] Yuki T, Keisuke F, Rikizo I, Takashi Y and Nobuyuki I 2016 *Phys. Rev. A* **93** 052307
[24] Sheng Y B and Zhou L 2018 *Phys. Rev. A* **98** 052343
[25] Xiao M, Liu L and Song X 2018 *Quantum Inf. Process.* **17** 63
[26] Tan X Q, Tao H, Zhang X Q, Zeng X D and Xu Q S 2021 *Quantum Inf. Process.* **20** 9