




## Verification of blind quantum computation with entanglement witnesses

Qingshan Xu , Xiaoqing Tan, \* Rui Huang , and Meiqi Li

*College of Information Science and Technology, Jinan University, Guangzhou 510632, China*

 (Received 31 March 2021; revised 24 September 2021; accepted 29 September 2021; published 12 October 2021)

Verifiable blind quantum computation provides a cloud scenario for scalable quantum information processing. However, constructing one resource-efficient verification protocol is still an open problem. In this paper, the context of verification we consider is the measurement-based model, in which the client receives the graph state prepared by the server and performs single-qubit measurements on it to drive the computation. We first utilize three entanglement witnesses to estimate the fidelity of the prepared graph state. Applying entanglement witnesses to design the test phase, we propose verification protocols. Our protocol requires overhead in terms of copies of the graph state that scales as  $O(n^2 \log n)$ , where  $n$  is the number of qubits of the graph state. Furthermore, the soundness of our protocol is improved. The advantages of our protocol are derived from the fact that each entanglement witness can be implemented by the client with a fixed number of measurement settings.

DOI: [10.1103/PhysRevA.104.042412](https://doi.org/10.1103/PhysRevA.104.042412)

### I. INTRODUCTION

Quantum computation has drawn intense interest in recent years due to the growing trend of quantum supremacy [1]. Quantum computers can efficiently solve problems which are intractable on classical computers. For instance, Shor's algorithm can achieve dramatic reductions in run time for integer factorization [2]. However, scalable quantum computation is still hard to achieve. The number of qubits in existing quantum computers is less than 100, which means that we are in the noise intermediate-scale era [3]. Quantum computing is likely to be implemented in the cloud model in the near future since quantum computing resources, such as graph states, are rare for a user. In the cloud environment, the user can access quantum computing capabilities remotely. Blind quantum computing (BQC) [4–18] provides such a cloud scheme, in which a client with only the ability to do classical computing and prepare or measure single qubits can delegate computation tasks to a server who has the ability to do universal quantum computation while simultaneously keeping the input, output, and algorithm unknown to the server. The first blind quantum computation protocol, in which the quantum circuit model was considered and a quantum one-time pad was used to encrypt input qubits, was proposed by Childs [4]. Afterward, the first blind quantum computation protocol using measurement-based quantum computing (MBQC) [19–21], in which the quantum ability that the client needs is preparing rotated single-qubit states, was proposed by Broadbent *et al.* [5]. The blind quantum computation protocol we consider in this paper was proposed by Morimae and Fuji [10] and is called measurement-only blind quantum computing. In their protocol, the server prepares a universal resource state of MBQC and sends each qubit of the resource state one by one to the client, who subsequently performs single-qubit measurements

on received qubits. From the perspective of quantum ability owned by the client, single-qubit measurement is much easier to implement than single-qubit state generation.

Universal blind quantum computation can guarantee the correctness and the blindness. In other words, if the server is honest, the client will obtain the correct outcome, and privacy is preserved. However, if the server is malicious, the client cannot make sure that the outcome sent by the server is correct. This has caused the need for a client to be able to verify the correctness of the computation outcome, which is called verification of blind quantum computation. There have been many verifiable blind quantum computation (VBQC) protocols [22–39] that can fully solve this problem. There are two main types of verification protocols. The first type is called trap-based verification [28,29], in which a client required to prepare single-qubit states embeds trap qubits in the computation to verify the behavior of the server. Based on this, several protocols achieving a completely classical client were proposed [24,26,30,38]. However, multiple non-communicating servers are required. The second type is called measurement-only verification [23,25,31–34,36], in which a client required to make single-qubit measurements directly verifies the resource state of MBQC sent by a server. In this paper, we focus on measurement-only verification and certify the graph state [40].

All proposed measurement-only verification protocols utilizing stabilizer testing [25,31,34,36] for the graph state have a large resource overhead. This is an obstacle to the development of scalable quantum computing. Here, we introduce the notion of entanglement witnesses [41–46] to VBQC. Entanglement witnesses have also been used in quantum key distribution for security proofs [47]. In the case of VBQC, the resource state or graph state is just in the form of entanglement. It is therefore a natural idea to utilize entanglement witnesses to verify the graph state. Compared with previous verification protocols, our protocol dramatically reduces the resource overhead.

\*ttanxq@jnu.edu.cn

The remainder of this paper is organized as follows. In Sec. II, we introduce the technical groundwork for entanglement witnesses to make an estimation of the fidelity. In Sec. III, we propose our VBQC protocols with respect to entanglement witnesses. In Sec. IV, we finally conclude our results and leave some open problems.

## II. ESTIMATING THE FIDELITY WITH ENTANGLEMENT WITNESSES

Recall that in measurement-only BQC, a client (Alice) receives a graph state prepared by a server (Bob) and performs single-qubit measurements to obtain the outcome she wants. The server cannot get any information about the client due to the no-signaling principle [48]. Since no message is sent from the client to the server, the no-signaling principle guarantees that if the client and the server share a system, the client cannot transmit any of her messages to the server regardless of what they do on their systems. We refer to this as blindness. However, a malicious server can prepare any state to destroy the computation so that the client gets the incorrect outcome. In order to achieve verifiability, Alice will instruct Bob to prepare a certain number of copies of the graph state (dishonest Bob may not obey orders). Alice then alternates performing the computation and testing the server's behavior. Bob has no knowledge about which copies of the graph state are used for testing and which are used for the ultimate computation task. If the test is passed, Alice can guarantee that the copy used for the computation task is close to the desired graph state. In this section we propose two methods using entanglement witnesses to estimate the fidelity between an unknown state and a given graph state, which will be used to design the above test of VBQC (see Sec. III).

Let us start by introducing entanglement witnesses of the graph state. Given an undirected graph  $G$  with  $n$  vertices  $i \in V$  and edges  $(i, j) \in E$ , the graph state  $|G\rangle$  that corresponds to  $G$  is defined by  $|G\rangle = (\prod_{(i,j) \in E} U_{ij})|+\rangle^{\otimes n}$ , where  $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  represents the state of each vertex and  $U_{ij}$  is the controlled- $Z$  gate  $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$  that acts on qubits corresponding to vertices  $i$  and  $j$ . Here,  $I$  is the identity operator, and  $Z$  is the Pauli matrix  $\sigma_z$ . The graph state  $|G\rangle$  has  $n$  stabilizers  $g_i = X_i \prod_{k \in N(i)} Z_k$  for  $i = 1, 2, \dots, n$ , where  $N(i)$  is the set of neighbors of vertex  $i$  and  $X_i$  and  $Z_i$  denote the Pauli matrices  $\sigma_x$  and  $\sigma_z$  acting on vertex  $i$ . The graph state  $|G\rangle$  is defined as the unique state fulfilling  $|G\rangle = g_i|G\rangle$  for all  $i$ . The term "entanglement witness" was introduced by Terhal [42]. An entanglement witness  $W$  is an observable such that (i)  $\text{Tr}(W\rho_s) \geq 0$  for all separable state  $\rho_s$  and (ii)  $\text{Tr}(W\rho_e) < 0$  for at least one entangled state  $\rho_e$ . Here,  $\text{Tr}(\cdot)$  represents the trace of the matrix. We therefore say that  $W$  detects the entanglement of  $\rho_e$ . A typical entanglement witness detecting genuine  $n$ -qubit entanglement for a state close to the  $n$ -qubit graph state  $|G\rangle$  is

$$W_1 = \frac{I}{2} - |G\rangle\langle G| = \frac{I}{2} - \prod_{i=1}^n \frac{g_i + I}{2}, \quad (1)$$

where the projector on the state to be detected has been used as an observable to detect entanglement (see Sec. 3.6.2 of Ref. [44]). See Sec. 3.4.3 of Ref. [44] for the second equality

of Eq. (1). The witness  $W_1$  should be decomposed into a sum of locally measurable operators for the convenience of measurements in an experiment. However, the number of local measurements in these decompositions probably increases exponentially with the number of qubits [49]. Hence, two types of witnesses with constant measurement settings have been proposed [50,51]. In order to explain these witnesses, we need to introduce the notion of the colorability of a graph. A graph is called  $m$ -colorable if all vertices of the graph can be divided into at least  $m$  disjoint subsets  $S_1, \dots, S_m$  of vertices, where there are no edges between any pair of vertices in  $S_j$  for any  $j$ . We say that  $S_1, \dots, S_m$  are  $m$  divided sets of the  $m$ -colorable graph. One of witnesses for the graph state  $|G\rangle$  corresponding to a two-colorable graph  $G$  is

$$W_2 = 3I - 2 \left[ \prod_{i \in S_1} \frac{g_i + I}{2} + \prod_{i \in S_2} \frac{g_i + I}{2} \right], \quad (2)$$

where  $S_1$  and  $S_2$  are two divided sets of the two-colorable graph  $G$ . Two-colorable graph states such as a brickwork state [5] and a Raussendorf-Harrington-Goyal (RHG) state [52] are widely used as the resource state of BQC. Generally, the  $m$ -colorable graph state  $|G\rangle$  has the witness

$$W_3 = 3I - 2 \sum_{j=1}^m \left( \prod_{i \in S_j} \frac{g_i + I}{2} \right), \quad (3)$$

where  $S_1, \dots, S_m$  are  $m$  divided sets of the  $m$ -colorable graph  $G$ . Another witness for the graph state  $|G\rangle$  is

$$W_4 = (n-1)I - \sum_{i=1}^n g_i. \quad (4)$$

The construction of witnesses  $W_1, W_2, W_3$ , and  $W_4$  comes from the following fact. To make the expectation value of the witness reach a minimum for the graph state  $|G\rangle$ , a full set of generators, i.e.,  $n$  stabilizers, is necessary [53]. The coefficient  $1/2$  of witness  $W_1$  is derived from  $\max_{|\phi\rangle} |\langle \phi | G \rangle|^2$ , where  $|\phi\rangle$  belongs to the set of biseparable states [49]. The coefficient of witness  $W_2$  or  $W_4$  is chosen such that there is a positive number  $\alpha$  satisfying that  $W_2 - \alpha W_1$  or  $W_4 - \alpha W_1$  is negative semidefinite. As we will see later, all eigenvalues of the matrix  $W_2 - 2W_1$  are zero, which means that  $W_2 - 2W_1$  can be negative semidefinite. Combining it with  $\text{Tr}(|G\rangle\langle G|W_1) = -1/2$ , one can obtain  $\text{Tr}[|G\rangle\langle G|(W_2 - 2W_1)] \leq 0$ , i.e.,  $\text{Tr}(|G\rangle\langle G|W_2) \leq -1$ . This means that  $W_2$  detects the graph state  $|G\rangle$ . Similarly,  $W_4$  detects the graph state  $|G\rangle$ . As for witness  $W_3$ , it is a generalization of witness  $W_2$  (see Sec. 6.6.2 of Ref. [44]).

According to the construction of witnesses  $W_3$  and  $W_4$ , they both need only  $m$  measurement settings for a given  $m$ -colorable graph state, where the  $j$ th measurement setting is the observable  $\prod_{i \in S_j} g_i$ . For example, three measurement settings needed for the three-colorable triangular lattice graph state [54] are illustrated in Fig. 1, where all vertices of the triangular lattice graph are divided into the subset  $S_1$  of red vertices, the subset  $S_2$  of green vertices, and the subset  $S_3$  of blue vertices.

As mentioned earlier, measuring the witnesses on the graph state  $|G\rangle$  can detect the entanglement of  $|G\rangle$ . If we measure the witnesses on the state used for the test stage, where the

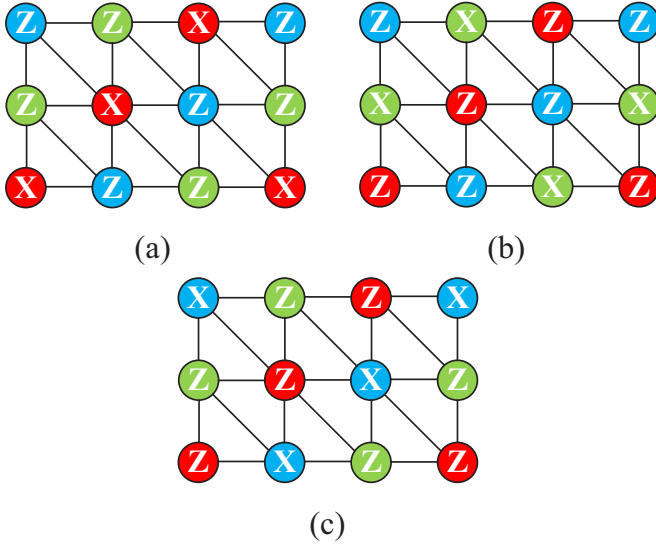


FIG. 1. Three measurement settings needed for the three-colorable triangular lattice graph state  $|G\rangle$ . (a) The observable  $\prod_{i \in S_1} g_i$  on  $|G\rangle$ . Alice measures red qubits in the  $X$  basis and other qubits in the  $Z$  basis. (b) The observable  $\prod_{i \in S_2} g_i$  on  $|G\rangle$ . Alice measures green qubits in the  $X$  basis and other qubits in the  $Z$  basis. (c) The observable  $\prod_{i \in S_3} g_i$  on  $|G\rangle$ . Alice measures blue qubits in the  $X$  basis and other qubits in the  $Z$  basis.

unknown state prepared by Bob is treated as  $|G\rangle$  to perform the measurement settings, we can determine whether or not the state used for the computation stage is close to  $|G\rangle$ . Thus, Bob's behavior is verified. To clarify this, we give our two methods for estimating the fidelity  $F = \langle G|\rho|G\rangle$  for an unknown state  $\rho$  once we get the real number  $\text{Tr}(W\rho)$  coming from local measurements. An approach for estimating fidelity is to construct the positive-semidefinite operator. This method has been used to estimate the fidelity between the prepared state and an ideal Greenberger-Horne-Zeilinger (GHZ) state or cluster state [53]. We generalize it to the case of the graph state. Let us explain our main idea. We need to find a positive number  $\alpha$  such that  $W - \alpha W_1 \geq 0$ , where  $\geq 0$  means that the operator is positive semidefinite. Then using the inequality  $\text{Tr}[(W - \alpha W_1)\rho] \geq 0$ , we get a lower bound on the fidelity from the expectation value of the witness  $W$ , i.e.,

$$F = \langle G|\rho|G\rangle \geq \frac{1}{2} - \frac{1}{\alpha} \text{Tr}(W\rho). \quad (5)$$

We consider exploring the existence of  $\alpha$  for  $W \in \{W_2, W_3, W_4\}$ . We start by introducing a special basis. The eigenvectors corresponding to the eigenvalues  $\pm 1$  of the stabilizers  $\{g_i\}_{i=1}^n$  form a complete basis of the  $n$ -qubit Hilbert space, which is similar to the GHZ basis in [53]. We call this basis the  $G$  basis. We then label the basis states with  $n$ -tuples of  $\{0, 1\}$ , i.e.,  $|\Phi_{00\dots 0}\rangle, |\Phi_{00\dots 1}\rangle, \dots, |\Phi_{11\dots 1}\rangle$ . The  $i$ th digit of the basis state  $|\varphi\rangle$  is 0 (1) if and only if  $\langle \varphi|g_i|\varphi\rangle = +1$  ( $-1$ ). For example, the graph state  $|G\rangle$  is the basis state  $|\Phi_{00\dots 0}\rangle$ , where the subscript tuple  $00\dots 0$  originates from the fact that  $\langle G|g_i|G\rangle = +1$  holds for all  $i$ . Let us observe the matrix forms of witnesses in the  $G$  basis. The matrix form of  $g_i$  in the  $G$  basis is  $I^{\otimes(i-1)} \otimes Z \otimes I^{\otimes(n-i)}$  since  $g_i$  gives  $+1$  and  $-1$  expectation values for states of the form  $|\Phi_{s_1\dots s_{i-1}0s_{i+1}\dots s_n}\rangle$  and

$|\Phi_{s_1\dots s_{i-1}1s_{i+1}\dots s_n}\rangle$ , respectively. Furthermore, the matrix forms of  $W_1, W_2, W_3$ , and  $W_4$  in the  $G$  basis can be written as

$$W_1^G = \text{diag}\left(-\frac{1}{2}, \frac{1}{2}, \dots, -\frac{1}{2}, \frac{1}{2}\right), \quad (6)$$

$$W_2^G = W_4^G = \text{diag}(-1, 1, \dots, -1, 1), \quad (7)$$

$$W_3^G = \text{diag}(3 - 2m, 5 - 2m, \dots, 3 - 2m, 5 - 2m), \quad (8)$$

where  $\text{diag}$  represents a diagonal matrix. Thus, we have  $W_2^G - 2W_1^G = 0$  and  $W_4^G - 2W_1^G = 0$ . According to linear algebra, the matrix  $W_2 - 2W_1$  is similar to the matrix  $W_2^G - 2W_1^G$ , which means that their eigenvalues are zero. Hence,  $W_2 - 2W_1 \geq 0$  is satisfied, i.e.,  $\alpha = 2$ .  $W_4 - 2W_1 \geq 0$  is obtained in an analogous way. However, when  $m \geq 3$ , there exists at least one negative number on the diagonal of matrix  $W_3^G - \alpha W_1^G$  for any  $\alpha$ , so that  $W_3 - \alpha W_1$  is not positive semidefinite. To this end, we have

$$F \geq \frac{1}{2} - \frac{1}{2} \text{Tr}(W_2\rho), \quad (9)$$

$$F \geq \frac{1}{2} - \frac{1}{2} \text{Tr}(W_4\rho). \quad (10)$$

If  $\rho$  is exactly the ideal graph state  $|G\rangle\langle G|$ , then  $\text{Tr}(W_2\rho) = \text{Tr}(W_4\rho) = -1$ . Consequently, both witnesses  $W_2$  and  $W_4$  can obtain the fidelity  $F = 1$ .

Another approach for estimating fidelity is inspired by estimating entanglement measures [55]. In the above background, one aims to derive

$$\varepsilon(W) = \inf_{\rho} \{E(\rho) | \text{Tr}(W\rho) = w\}, \quad (11)$$

where  $E(\cdot)$  is some entanglement measure or another convex and continuous function and  $w$  is the mean value for measuring the witness  $W$ . Note that  $\varepsilon(W)$  is actually the infimum of  $E(\rho)$  over all states compatible with the data  $\text{Tr}(W\rho) = w$ . Using the Legendre transform [56] of the entanglement measure  $E$ , one can get

$$\varepsilon(W) = \sup_r \{r w - \hat{E}(rW)\}, \quad (12)$$

where  $r$  is an arbitrary real number,  $\hat{E}(rW) = \sup_{|\psi\rangle} \{\langle \psi | rW | \psi \rangle - E(|\psi\rangle)\}$ , and  $|\psi\rangle$  is an arbitrary pure state.

Here, we use  $E(\cdot) \in [0, 1]$  to denote the fidelity, i.e.,  $E(\cdot) = \langle G | \cdot | G \rangle$ . Then we have  $\hat{E}(rW) = \sup_{|\psi\rangle} \{\langle \psi | (rW - |G\rangle\langle G|) | \psi \rangle\}$ . The supremum is obtained when  $|\psi\rangle$  is the eigenvector for the largest eigenvalue of  $rW - |G\rangle\langle G|$ . Let us consider the case of  $W = W_3$ . First, the matrix form of  $rW_3 - |G\rangle\langle G|$  in the  $G$  basis can be expressed as

$$\text{diag}(r(3 - 2m) - 1, r(5 - 2m), \dots, r(3 - 2m) - 1, r(5 - 2m)) \quad (13)$$

Since the eigenvalues of the matrix form of the same operator in different bases are invariant, the eigenvalues of  $rW_3 - |G\rangle\langle G|$  are  $r(3 - 2m) - 1$  and  $r(5 - 2m)$ . This means  $\hat{E}(rW_3) = \max\{r(3 - 2m) - 1, r(5 - 2m)\}$ . If  $\rho$  is exactly the ideal graph state  $|G\rangle\langle G|$ , then  $\text{Tr}(W_3\rho) = 3 - 2m$ .

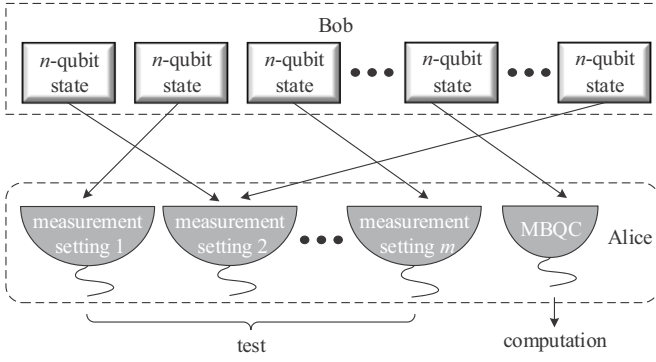


FIG. 2. Illustration of the verification of BQC with entanglement witnesses. Bob prepares a quantum state that consists of a number of registers, where each register consists of an  $n$ -qubit state, and sends it to Alice. If Bob is honest, the state of each register is the ideal  $m$ -colorable graph state  $|G\rangle$ . However, if Bob is malicious, registers could be entangled with each other. Alice randomly chooses a register to perform MBQC that is used for computation tasks. For the remaining registers for the test phase, each register is measured in one measurement setting that is selected randomly. If the measurement outcomes in the test satisfy certain conditions, the state of the register used for computation will be close to  $|G\rangle$ .

Furthermore, we have

$$\begin{aligned}
 E(\varrho) &\geq \sup_r \{r \text{Tr}(W_3 \varrho) - \hat{E}(rW_3)\} \\
 &= \begin{cases} \sup_r \{r(3-2m) - [r(3-2m)-1]\} = 1, & r < -1/2 \\ \sup_r \{-2r\}, & r \geq -1/2 \end{cases} \\
 &= 1;
 \end{aligned} \tag{14}$$

that is, the fidelity satisfies  $F = 1$ . If  $\varrho$  deviates slightly from the ideal graph state, then  $\text{Tr}(W_3 \varrho) = 3 - 2m + \delta$ , where  $\delta > 0$  is small enough. Similarly, we have

$$\begin{aligned}
 E(\varrho) &\geq \sup_r \{r \text{Tr}(W_3 \varrho) - \hat{E}(rW_3)\} \\
 &= \begin{cases} \sup_r \{1 + r\delta\}, & r < -1/2 \\ \sup_r \{-2r + r\delta\}, & r \geq -1/2 \end{cases} \\
 &= 1 - \delta/2.
 \end{aligned} \tag{15}$$

In order to figure out how one can use the estimation of the fidelity in this section to complete the verification of blind quantum computation, let us focus on the process of verification of BQC, which is shown in Fig. 2. Note that the measurement settings in the test phase are used to collect statistics corresponding to entanglement witnesses. Owing to the techniques of probability theory, the outcomes derived from the  $j$ th measurement setting on the registers used for test can be used to estimate the outcomes of the  $j$ th measurement setting on the  $n$ -qubit state  $\rho_{\text{MBQC}}$  used for computation. And then one can calculate the value  $\text{Tr}(W \rho_{\text{MBQC}})$  for any witness  $W \in \{W_2, W_3, W_4\}$ . Utilizing expressions (9), (10), and (15) of the estimation of the fidelity given in this section, we finally obtain a lower bound of the fidelity of the state  $\rho_{\text{MBQC}}$ .

If we require the measurement outcomes in the test phase to satisfy certain conditions, then the fidelity  $\langle G | \rho_{\text{MBQC}} | G \rangle$  will approach 1. Therefore, we achieve the verification of the resource state of blind quantum computation.

### III. VERIFIABLE BLIND QUANTUM COMPUTATION WITH ENTANGLEMENT WITNESSES

In this section, we use the estimation of the fidelity in Sec. II, Serfling's bound [57], and the Azuma-Hoeffding bound [58] to analyze verifiable properties of our protocols. The properties that we consider are completeness and soundness. The completeness means a high joint probability that when Bob is honest, Alice accepts the result and the outcome is correct. The soundness means a low conditional probability of obtaining an incorrect outcome given that Alice accepts the result. The soundness says that when Alice accepts the result, there is a high probability for the state prepared by Bob to be close to the ideal graph state.

Before proceeding, we first clarify Serfling's bound and the Azuma-Hoeffding bound so that one can prove the verifiability of the protocol.

*Lemma 1. Serfling's bound.* Given a set of  $T$  binary random variables  $Y = (Y_1, Y_2, \dots, Y_T)$  with  $Y_k \in \{0, 1\}$  and two arbitrary positive integers  $N$  and  $K$  that satisfy  $T = N + K$ , we have

$$\begin{aligned}
 \Pr \left( \sum_{k \in \bar{\Pi}} Y_k \leq \frac{N}{K} \sum_{k \in \Pi} Y_k + Nv \right) \\
 \geq 1 - \exp \left( - \frac{2v^2 N K^2}{(N+K)(K+1)} \right)
 \end{aligned} \tag{16}$$

for any  $0 < v < 1$ , where  $\Pr(\cdot)$  denotes the event probability,  $\Pi$  is a set of  $K$  samples chosen independently and uniformly at random from  $Y$  without replacement, and  $\bar{\Pi}$  is the complementary set of  $\Pi$  in  $Y$ .

*Lemma 2. Azuma-Hoeffding bound.* Let  $\xi_1, \xi_2, \dots, \xi_n$  be independent random variables, where  $\xi_i \in [a_i, b_i]$ ,  $i = 1, 2, \dots, n$ . We have that for any  $t > 0$ ,

$$\begin{aligned}
 \Pr \left[ \frac{\xi_1 + \xi_2 + \dots + \xi_n}{n} - \mathbb{E} \left( \frac{\xi_1 + \xi_2 + \dots + \xi_n}{n} \right) \leq t \right] \\
 \geq 1 - \exp \left( - \frac{2n^2 t^2}{\sum_{i=1}^n (b_i - a_i)^2} \right),
 \end{aligned} \tag{17}$$

where  $\mathbb{E}(\cdot)$  is the mathematical expectation.

Let us first focus on the scenario for the witness  $W_2$ . We define a random variable  $M_j^\varrho \in \{0, 1\}$  in the case of performing the  $j$ th measurement setting on an arbitrary  $n$ -qubit state  $\varrho$ . More precisely, we define

$$M_j^\varrho = \prod_{i \in S_j} \frac{x_i \prod_{k \in N(i)} z_k + 1}{2}, \tag{18}$$

where  $x_i \in \{-1, 1\}$  and  $z_k \in \{-1, 1\}$  are the measurement outcomes of Pauli observables  $X_i$  and  $Z_k$  acting on the state  $\varrho$ ,



respectively. Thus, we have

$$\text{Tr}\left(\prod_{i \in S_j} \frac{g_i + I}{2} \rho\right) = \overline{M_j^\rho}, \quad (19)$$

where  $\overline{M_j^\rho}$  is the mathematical expectation of the random variable  $M_j^\rho$ . Our verification protocol using the witness  $W_2$  is shown in Protocol 1.

**Protocol 1** Verifiable blind quantum computation with witness  $W_2$ .

**Step 1.**

Honest Bob prepares a  $3Kn$ -qubit state  $|G\rangle^{\otimes 3K}$  and sends each of its qubits one by one to Alice, where  $|G\rangle$  is an  $n$ -qubit graph state on a two-colorable graph  $G$ . Here,  $K$  is set to be  $\lceil n^2 \log n \rceil$ , where  $\lceil \cdot \rceil$  is the ceiling function. However, malicious Bob can prepare any  $3Kn$ -qubit state  $\rho_{\text{Bob}}$ . Whether or not Bob is honest, Alice sequentially divides the state sent by Bob into  $3K$  registers, where each register stores  $n$  qubits.

**Step 2.**

Alice repeats the following local measurements for  $1 \leq j \leq 2$ : Alice chooses  $K$  registers from the remaining  $(4 - j)K$  registers independently and uniformly at random, and then she performs the  $j$ th measurement setting on the  $K$  registers that are chosen. More specifically, for each selected register, Alice measures in Pauli observable  $X$  the qubits corresponding to the divided set  $S_j$  of the two-colorable graph  $G$  and other qubits in Pauli observable  $Z$ . Alice then calculates the value  $M_j^\rho$  according to Eq. (18). We denote the number of registers satisfying  $M_j^\rho = 0$  as  $K_j$ .

**Step 3.**

Alice uses one register chosen from the remaining  $K$  registers uniformly at random for computational tasks and discards the other  $K - 1$  registers. The chosen single register is called the target register, and the averaged state of the target register is  $\rho_{\text{tgt}} = \frac{1}{K} \sum_{i=1}^K \rho_i$ , where  $\rho_i$  is the state of the  $i$ th register of the remaining  $K$  registers.

**Step 4.**

Alice accepts the result of the computation performed on the target register if

$$K_1 + K_2 \leq \frac{K}{2n}. \quad (20)$$

The main reason why the accepting condition in step 4 is taken to be Eq. (20) is as follows. We need to keep the scale of the fidelity  $\langle G | \rho_{\text{tgt}} | G \rangle$  of Protocol 1 as  $1 - O(1/n)$  for the comparison with the soundness of Ref. [36]. As mentioned in Appendix A, the fidelity is given by Eq. (A10). In other words, the fidelity satisfies  $\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - 3v - 2t - 2(K_1 + K_2)/K$  for any  $0 < v < 1$  and  $t > 0$  with a probability of at least  $[1 - \exp(-v^2 K/2)]^2 [1 - \exp(-2Kt^2)]^2$ . If we set  $v = O(1/n)$ ,  $t = O(1/n)$ ,  $K_1 + K_2 \leq K/2n$ , then  $\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - O(1/n)$  is obtained. The reason why the overhead of Protocol 1 is  $O(n^2 \log n)$  copies of the graph state is as follows. Since the required number of graph states is  $3K$ , the overhead depends on the parameter  $K$ . In order to make the above confidence probability scale as  $1 - O(n^{-\lambda})$  for a certain constant  $\lambda$ ,  $K$  should be chosen to be  $O(n^2 \log n)$ .

Now we show how to derive the completeness and soundness of Protocol 1. In order to see the completeness, we consider the case that Bob behaves honestly. We need to calculate the probability that Alice accepts the result and the probability that the result coming from the target register is correct. The product of both probabilities is the completeness. One can see that if Bob is honest in Protocol 1, he will prepare  $|G\rangle^{\otimes 3K}$ . In other words, the state of every register is  $|G\rangle\langle G|$ . According to Eq. (19),  $\overline{M_j^\rho} = 1$  holds for every register used for the  $j$ th measurement setting in step 2. This implies that all registers satisfy  $M_j^\rho = 1$  for the process of performing the  $j$ th measurement setting on the  $K$  registers, i.e.,  $K_1 = K_2 = 0$ . Since the accepting condition (20) is always satisfied, there is a unit probability that Alice accepts the result. In addition, the target register is prepared in the form of the ideal graph state  $|G\rangle$ . Hence, the probability that the result coming from the target register is correct is 100%. Finally, the completeness of Protocol 1 can be obtained, which is a unit probability. In the case of soundness, we have the following theorem.

*Theorem 1.* Assume that  $\lambda_1$  is any constant satisfying  $\log_n 16 < \lambda_1 < (n - 1)^2/16$  and  $n \geq 6$ . If Protocol 1 is accepted, we can guarantee that the  $n$ -qubit averaged state  $\rho_{\text{tgt}}$  satisfies, with a probability of at least  $1 - 4n^{-\lambda_1/2}$ ,

$$\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - \frac{1 + 4\sqrt{\lambda_1}}{n}. \quad (21)$$

*Proof.* Using Lemma 1, we first show that if we perform the  $j$ th measurement setting on the final  $K$  registers of step 3 in Protocol 1, then an upper bound of the number of registers satisfying  $M_j^\rho = 0$  and the relevant confidence probability can be obtained. Hence, the lower bound of  $\sum_{k=1}^K M_j^{\rho_k}$  is directly given. Using Lemma 2, we then get a lower bound of  $\frac{1}{K} \sum_{k=1}^K \overline{M_j^{\rho_k}}$  and the relevant confidence probability. Starting from Eq. (19), we can obtain a lower bound of  $\text{Tr}(\prod_{i \in S_j} \frac{g_i + I}{2} \rho_{\text{tgt}})$ . According to the estimation (9) of the fidelity and the expression (2) of witness  $W_2$ , we finally prove that the fidelity  $\langle G | \rho_{\text{tgt}} | G \rangle$  satisfies a lower bound with a certain confidence probability. The full proof is given in Appendix A.

Protocol 1 offers a large improvement over current verification protocols. The protocol of Takeuchi *et al.* [36] considered stabilizer testing and Serfling's bound. They guarantee the fidelity  $1 - (2\sqrt{c} + 1)/n$  with a probability of at least  $1 - n^{1-5c/64}$ , where  $c$  is any constant satisfying  $64/5 < c < (n - 1)^2/4$  and  $n \geq 9$ . However, the number of total copies of the graph state  $|G\rangle$  is  $O(n^5 \log n)$  in their protocol. Note that Protocol 1 needs only  $O(n^2 \log n)$  copies of the graph state. In addition, the soundness of Protocol 1 is better than that of Ref. [36]. To clarify this, if we require the protocol of Ref. [36] to achieve the same fidelity as Protocol 1,

$$1 - \frac{1 + 4\sqrt{\lambda_1}}{n} = 1 - \frac{1 + 2\sqrt{c}}{n} \quad (22)$$

implies that  $c = 4\lambda_1$ . Furthermore,

$$1 - 4n^{-\lambda_1/2} > 1 - n^{1-5\lambda_1/16} \quad (23)$$

means that Protocol 1 has a better significance level.

Let us now turn to the scenario for witness  $W_4$ . We define one surjection  $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, m\}$  such that  $i \in$

$S_{f(i)}$ . Next, we define a random variable  $M_l^\rho \in \{-1, 1\}$  for any  $l \in S_j$  in the case of performing the  $j$ th measurement setting on an arbitrary  $n$ -qubit state  $\rho$ . More precisely, we define

$$M_l^\rho = x_l \prod_{k \in N(l)} z_k, \quad (24)$$

where  $x_l \in \{-1, 1\}$  and  $z_k \in \{-1, 1\}$  are the measurement outcomes of Pauli observables  $X_l$  and  $Z_k$  acting on the state  $\rho$ , respectively. Thus, we have

$$\text{Tr}(g_l \rho) = \overline{M_l^\rho}, \quad (25)$$

where  $\overline{M_l^\rho}$  is the mathematical expectation of the random variable  $M_l^\rho$ . Our verification protocol using witness  $W_4$  is described in Protocol 2.

---

**Protocol 2** Verifiable blind quantum computation with witness  $W_4$ .

---

**Step 1.**

Honest Bob prepares an  $[(m+1)Kn]$ -qubit state  $|G\rangle^{\otimes(m+1)K}$  and sends each of its qubits one by one to Alice, where  $|G\rangle$  is an  $n$ -qubit graph state on an  $m$ -colorable graph  $G$ . Here,  $K$  is set to be  $\lceil n^4 \log n \rceil$ . However, malicious Bob can prepare any  $[(m+1)Kn]$ -qubit state  $\rho_{\text{Bob}}$ . Whether or not Bob is honest, Alice sequentially divides the state sent by Bob into  $(m+1)K$  registers, where each register stores  $n$  qubits.

**Step 2.**

Alice repeats the following local measurements for  $1 \leq j \leq m$ : Alice chooses  $K$  registers from the remaining  $(m+2-j)K$  registers independently and uniformly at random, and then she performs the  $j$ th measurement setting on the  $K$  registers that are chosen. For any  $l \in S_j$ , we denote the number of registers satisfying  $M_l^\rho = -1$  as  $K_{jl}$ .

**Step 3.**

Follow step 3 of Protocol 1.

**Step 4.**

Alice accepts the result of the computation performed on the target register if

$$\max_j \left( \max_{l \in S_j} K_{jl} \right) \leq \frac{K}{n^2 m}. \quad (26)$$


---

The main reason why the accepting condition in step 4 is taken to be Eq. (26) is similar to that for Protocol 1. As mentioned in Appendix B, the fidelity is given by Eq. (B6). In other words, the fidelity satisfies  $\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - nmv - nt/2 - nm(\max_j \max_{l \in S_j} K_{jl})/K$  for any  $0 < v < 1$  and  $t > 0$  with a probability of at least  $[1 - \exp(-v^2 K/2)]^m [1 - \exp(-2Kt^2)]^m$ . If we set  $v = O(1/n^2)$ ,  $t = O(1/n^2)$ ,  $K_{jl} \leq K/n^2 m$  for all  $j$  and  $l \in S_j$ , then  $\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - O(1/n)$  is obtained. In order to make the above confidence probability scale as  $1 - O(n^{-\lambda})$  for a certain constant  $\lambda$ ,  $K$  should be chosen to be  $O(n^4 \log n)$ .

Similarly, the completeness of Protocol 2 is 100% since honest Bob always prepares  $|G\rangle^{\otimes(m+1)K}$  and  $K_{jl} = 0$  holds with unit probability for all  $l, j$ . The soundness of Protocol 2 is given by the following theorem.

*Theorem 2.* Assume that  $\lambda_2$  is any constant satisfying  $2 + \log_n 4 < \lambda_2 < (\frac{n-1}{1/2+m})^2$ . If Protocol 2 is accepted, we can guarantee that the  $n$ -qubit averaged state  $\rho_{\text{tgt}}$  satisfies, with a probability of at least  $1 - 2n^{1-\lambda_2/2}$ ,

$$\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - \frac{1 + (1/2 + m)\sqrt{\lambda_2}}{n}. \quad (27)$$

*Proof.* Using Lemma 1, we first show that if we perform the  $j$ th measurement setting on the final  $K$  registers of step 3 in Protocol 2, then there will be an upper bound of the number of registers satisfying  $M_l^\rho = -1$  and the relevant confidence probability for any  $l \in S_j$ . Using Lemma 2, we then get a lower bound of  $\frac{1}{K} \sum_{k=1}^K \overline{M_l^{\rho_k}}$  and the relevant confidence probability. Starting from Eq. (25), one can obtain a lower bound of  $\text{Tr}(g_l \rho_{\text{tgt}})$ . According to the estimation (10) of the fidelity and the expression (4) of witness  $W_4$ , we finally prove that the fidelity  $\langle G | \rho_{\text{tgt}} | G \rangle$  satisfies a lower bound with a certain confidence probability. The full proof is given in Appendix B.

In contrast to Ref. [36], Protocol 2 requires only  $O(n^4 \log n)$  copies of the graph state. Similarly, if we require the protocol of Ref. [36] to achieve the same fidelity as Protocol 2,

$$1 - \frac{1 + (1/2 + m)\sqrt{\lambda_2}}{n} = 1 - \frac{1 + 2\sqrt{c}}{n} \quad (28)$$

leads to  $c = (1/2 + m)^2 \lambda_1 / 4$ . Furthermore, when  $n \geq 16$  and  $m \leq 4$ ,

$$1 - 2n^{1-\lambda_2/2} > 1 - n^{1-5(1/2+m)^2 \lambda_2 / 256} \quad (29)$$

shows that Protocol 2 has a better significance level.

Let us consider the scenario for witness  $W_3$ . We introduce the same definition of the random variable  $M_j^\rho \in \{0, 1\}$  as in the scenario for witness  $W_2$ . Our verification protocol using witness  $W_3$  is shown in Protocol 3.

---

**Protocol 3** Verifiable blind quantum computation with witness  $W_3$ .

---

**Step 1.**

Follow step 1 of Protocol 2, where  $K$  is set to be  $\lceil 4m^2 n^2 \log n \rceil$ .

**Step 2.**

Follow step 2 of Protocol 2, where we denote the number of registers satisfying  $M_j^\rho = 0$  as  $K_j$ .

**Step 3.**

Follow step 3 of Protocol 1.

**Step 4.**

Alice accepts the result of the computation performed on the target register if

$$\sum_{j=1}^m K_j \leq \frac{K}{mn}. \quad (30)$$


---

The accepting condition (30) in step 4 is derived from the following fact. As described in Appendix C, the fidelity satisfies  $F > 1 - m^2 v - mt - m \sum_{j=1}^m K_j / K$  for any  $0 < v < 1$  and  $t > 0$  with a probability of at least  $[1 - \exp(-v^2 K/2)]^m [1 - \exp(-2Kt^2)]^m$ . If we set  $v =$

$O(1/n)$ ,  $t = O(1/n)$ ,  $\sum_{j=1}^m K_j \leq K/mn$ , then  $\langle G|\rho_{\text{tgt}}|G \rangle \geq 1 - O(1/n)$  is obtained. In order to make the above confidence probability scale as  $1 - O(n^{-\lambda})$  for a certain constant  $\lambda$ ,  $K$  should be chosen to be  $O(n^2 \log n)$ .

Note that if Bob is honest, the state received by Alice is  $|G\rangle^{\otimes(m+1)K}$  and  $K_j = 0$  holds with unit probability for all  $j$ . This implies that the completeness of Protocol 3 is 100%. In addition, we have derived the following theorem.

**Theorem 3.** Assume that  $\lambda_3$  is any constant satisfying  $2 \log_n 2m < \lambda_3 < (\frac{n-1}{m/2+1/4})^2$ . If Protocol 3 is accepted, we can guarantee that the  $n$ -qubit averaged state  $\rho_{\text{tgt}}$  satisfies, with a probability of at least  $1 - 2mn^{-\lambda_3/2}$ ,

$$\langle G|\rho_{\text{tgt}}|G \rangle \geq 1 - \frac{1 + (m/2 + 1/4)\sqrt{\lambda_3}}{n}. \quad (31)$$

*Proof.* The proof follows closely certain steps of the proof of Theorem 1. The difference is that  $j = 1, 2$  is replaced with  $j = 1, 2, \dots, m$ . Due to the estimation (15) of the fidelity and the expression (3) of witness  $W_3$ , we can prove that the fidelity  $\langle G|\rho_{\text{tgt}}|G \rangle$  satisfies a lower bound with a certain confidence probability. The full proof is given in Appendix C.

Compared with Ref. [36], Protocol 3 requires only  $O(n^2 \log n)$  copies of the graph state. Similarly, if we require the protocol of Ref. [36] to achieve the same fidelity as Protocol 3,

$$1 - \frac{1 + (m/2 + 1/4)\sqrt{\lambda_3}}{n} = 1 - \frac{1 + 2\sqrt{c}}{n} \quad (32)$$

leads to  $c = (m/2 + 1/4)^2 \lambda_3 / 4$ . Furthermore, when  $n \geq 18$  and  $m \leq 9$ ,

$$1 - 2mn^{-\lambda_3/2} > 1 - n^{1-5(m/2+1/4)^2 \lambda_3 / 256} \quad (33)$$

shows that Protocol 3 has a better significance level.

Let us give two numerical examples to compare intuitively the soundness of our protocols with Ref. [36]. We first consider that the number of qubits of the graph state is 50 and the graph state used in Protocol 2 and Protocol 3 is three-colorable, i.e.,  $n = 50, m = 3$ . According to Eqs. (21), (27), and (31), the comparison is shown in Fig. 3(a). The result indicates that the fidelity of our strategies is higher than that of Ref. [36] when the confidence probability is the same. In Fig. 3(b) we plot the case of  $n = 500, m = 2$ . Note that the fidelity of the traditional method can approach 0.98 with almost 100% confidence probability. Relatively speaking, there is a high confidence probability that the fidelity of Protocol 3 will reach 0.995.

Obviously, observing all our protocols shows that Protocol 3 is optimal because the graph state used in Protocol 3 can be any-colorable and the overhead is minimal. In fact, most of graph states used for MBQC are two-colorable or three-colorable, and the number  $n$  of qubits required for MBQC is usually large enough. The number  $n$  depends on the specific computing task and the graph state. For example, if we intend to implement the four-qubit SWAP gate on the cluster state, then 57 qubits are required [59]. Generally speaking, hundreds of qubits are necessary for complex tasks. We have already considered this point in previous analysis comparing our protocols with Ref. [36]. It is thus interesting to note that our protocols are applicable for verifying a quantum computation task in practice. Furthermore, our protocols can be made

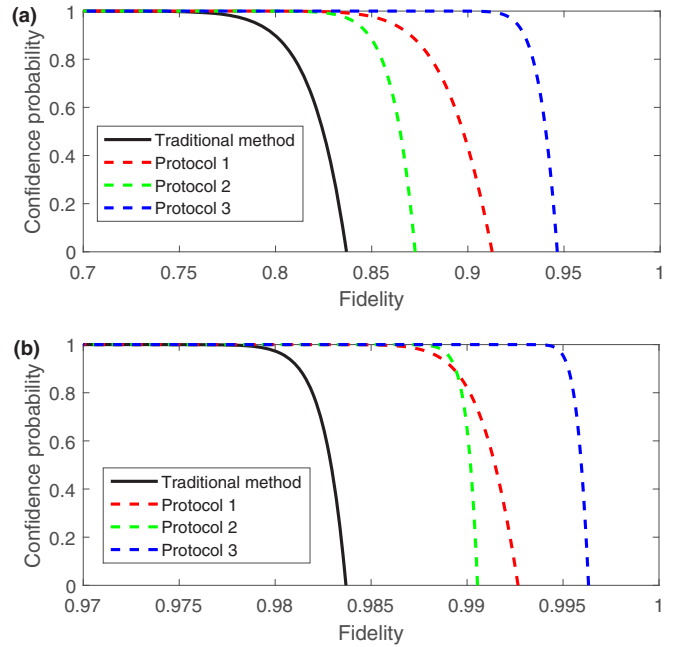


FIG. 3. The soundness of our strategies compared with the traditional method introduced in Ref. [36] for (a)  $n = 50, m = 3$  and (b)  $n = 500, m = 2$ . The soundness is shown by the confidence probability as a function of the fidelity. Interestingly, our protocols lead to a better soundness than the traditional method.

robust to noise by encoding graph states with a topological error correcting code [31,52].

#### IV. CONCLUSIONS

We have applied entanglement witnesses to design verifiable blind quantum computation protocols. To do so, we have shown that the fidelity of the prepared graph state can be estimated from the measured expectation values of entanglement witnesses. With the help of the estimation of the fidelity, verification protocols corresponding to different entanglement witnesses have been proposed. Finally, we have demonstrated the completeness and soundness for our protocols. For all we know, the most efficient VBQC protocol using the verification of the graph state is the protocol of Ref. [36], whose overhead in terms of the copies of the graph state is  $O(n^5 \log n)$ . In contrast to their protocol, the protocol described in this paper requires an overhead that scales as  $O(n^2 \log n)$ . In addition, the soundness of our protocol is better than that in Ref. [36]. The main reason is that the copies of the graph state required for different stabilizer tests in Ref. [36] do not overlap. This leads to extra overhead that is dependent on the number  $n$  of stabilizer tests. However, our method has removed it since the extra overhead caused by implementing the entanglement witnesses is related to the number of measurement settings, which is a constant number irrelevant to the size  $n$  of the graph state.

Although we have focused on the task of verifying graph states, one could consider entanglement witnesses for hypergraph states [60] or continuous-variable graph states [61] to extend the verification of quantum states. Recently, the trap-based verification protocols in Ref. [38] achieved

quasilinear resources, where a classical client interacts with noncommunicating servers that share entanglement. It is meaningful to bring the technology of entanglement witnesses to trap-based verification. Exploring these directions might help us to further construct efficient VBQC protocols.

### ACKNOWLEDGMENTS

This research is partly supported by the Natural Science Foundation of Guangdong Province of China under Grant No. 2021A1515011440, the Major Program of Guangdong Basic and Applied Research under Grant No. 2019B030302008, and the National Natural Science Foundation of China under Grant No. 62032009.

### APPENDIX A: PROOF OF THEOREM 1

Let us look back at Protocol 1. For the process of performing the first measurement setting on the  $K$  registers, we define the set  $\Pi^{(1)}$  to be the set which consists of these registers, and the set consisting of the remaining  $2K$  registers is denoted as  $\overline{\Pi}^{(1)}$ . If we set  $T = 3K$ ,  $N = 2K$ , and

$$Y_k = \begin{cases} 0, & M_1^{\rho'_k} = 1 \\ 1, & M_1^{\rho'_k} = 0 \end{cases} \quad (\text{A1})$$

in Lemma 1, where  $\rho'_k$  is the quantum state of the  $k$ th register in  $\Pi^{(1)}$  or  $\overline{\Pi}^{(1)}$  depending on  $k \in \Pi^{(1)}$  or  $k \in \overline{\Pi}^{(1)}$ , we can derive

$$\Pr\left(\sum_{k \in \overline{\Pi}^{(1)}} Y_k \leq \frac{2K}{K} \sum_{k \in \Pi^{(1)}} Y_k + 2Kv\right) \geq 1 - \exp\left(-\frac{2v^2 2KK^2}{(2K+K)(K+1)}\right). \quad (\text{A2})$$

This implies that once the first measurement setting is performed on the remaining  $2K$  registers, the maximal number of registers satisfying  $M_1^\rho = 0$  is  $2 \sum_{k \in \Pi^{(1)}} Y_k + 2Kv$  in the set  $\overline{\Pi}^{(1)}$ . Similarly, for the process of performing the second measurement setting on  $K$  registers, we define the set  $\Pi^{(2)}$  to be the set which consists of these registers, and the set consisting of the remaining  $K$  registers is denoted as  $\overline{\Pi}^{(2)}$ . If we set  $T = 2K$ ,  $N = K$ , and

$$Y_k = \begin{cases} 0, & M_2^{\rho'_k} = 1 \\ 1, & M_2^{\rho'_k} = 0 \end{cases} \quad (\text{A3})$$

in Lemma 1, where  $\rho'_k$  is the quantum state of the  $k$ th register in  $\Pi^{(2)}$  or  $\overline{\Pi}^{(2)}$  depending on  $k \in \Pi^{(2)}$  or  $k \in \overline{\Pi}^{(2)}$ , we can obtain

$$\Pr\left(\sum_{k \in \overline{\Pi}^{(2)}} Y_k \leq \frac{K}{K} \sum_{k \in \Pi^{(2)}} Y_k + Kv\right) \geq 1 - \exp\left(-\frac{2v^2 KK^2}{(K+K)(K+1)}\right). \quad (\text{A4})$$

This means that once the second measurement setting is performed on the remaining  $K$  registers, the maximal number of registers satisfying  $M_2^\rho = 0$  is  $\sum_{k \in \Pi^{(2)}} Y_k + Kv$  in the set  $\overline{\Pi}^{(2)}$ .

According to the above analysis, if we perform the first measurement setting on the final  $K$  registers that are not measured, then there are at least  $K - (2 \sum_{k \in \Pi^{(1)}} Y_k + 2Kv)$  registers satisfying  $M_1^\rho = 1$ , i.e.,

$$\sum_{k=1}^K M_1^{\rho_k} \geq K - \left(2 \sum_{k \in \Pi^{(1)}} Y_k + 2Kv\right). \quad (\text{A5})$$

In addition, if we perform the second measurement setting on the final  $K$  registers that are not measured, we have

$$\sum_{k=1}^K M_2^{\rho_k} \geq K - \left(\sum_{k \in \Pi^{(2)}} Y_k + Kv\right). \quad (\text{A6})$$

Using Lemma 2, we get

$$\Pr\left(\frac{1}{K} \sum_{k=1}^K M_1^{\rho_k} - \frac{1}{K} \sum_{k=1}^K \overline{M_1^{\rho_k}} < t\right) \geq 1 - \exp(-2Kt^2). \quad (\text{A7})$$

Relations (19) and (A5) allow us to transform this into

$$\Pr\left[\text{Tr}\left(\prod_{i \in S_1} \frac{g_i + I}{2} \rho_{\text{tgt}}\right) > 1 - \frac{1}{K} \left(2 \sum_{k \in \Pi^{(1)}} Y_k + 2Kv\right) - t\right] \geq 1 - \exp(-2Kt^2). \quad (\text{A8})$$

Similarly, we have

$$\Pr\left[\text{Tr}\left(\prod_{i \in S_2} \frac{g_i + I}{2} \rho_{\text{tgt}}\right) > 1 - \frac{1}{K} \left(\sum_{k \in \Pi^{(2)}} Y_k + Kv\right) - t\right] \geq 1 - \exp(-2Kt^2). \quad (\text{A9})$$

Using the estimation (9) of the fidelity in Sec. II, it follows that

$$\begin{aligned} F &\geq \frac{1}{2} - \frac{1}{2} \text{Tr}(W_2 \rho_{\text{tgt}}) \\ &\geq -1 + \sum_{j=1}^2 \text{Tr}\left(\prod_{i \in S_j} \frac{g_i + I}{2} \rho_{\text{tgt}}\right) \\ &\geq 1 - 3v - 2t - \frac{1}{K} \left(2 \sum_{k \in \Pi^{(1)}} Y_k + \sum_{k \in \Pi^{(2)}} Y_k\right) \\ &\geq 1 - 3v - 2t - \frac{2}{K} \left(\sum_{j=1}^2 \sum_{k \in \Pi^{(j)}} Y_k\right), \end{aligned} \quad (\text{A10})$$

where  $F = \langle G | \rho_{\text{tgt}} | G \rangle$ , and the second inequality and the third inequality are obtained from Eqs. (2) and (A8) and (A9), respectively. In addition, we can guarantee that Eq. (A10) is



established with probability

$$\begin{aligned}
 P &\geq \left[ 1 - \exp\left(-2v^2K \frac{2}{3(1+1/K)}\right) \right] \left[ 1 - \exp\left(-v^2K \frac{1}{1+1/K}\right) \right] [1 - \exp(-2Kt^2)]^2 \\
 &\geq \left[ 1 - \exp\left(-\frac{1}{2}v^2K\right) \right]^2 [1 - \exp(-2Kt^2)]^2.
 \end{aligned} \tag{A11}$$

Let us set  $v = \sqrt{\lambda_1}/n$  and  $t = \sqrt{\lambda_1}/(2n)$ , where  $\lambda_1$  is any constant satisfying  $\log_n 16 < \lambda_1 < (n-1)^2/16$  and  $n \geq 6$ . Combining this with the condition (20) of accepting, we conclude that the fidelity satisfies

$$F \geq 1 - \frac{1 + 4\sqrt{\lambda_1}}{n} \tag{A12}$$

with probability

$$P \geq \left[ 1 - \exp\left(-\frac{\lambda_1}{2n^2}n^2 \log n\right) \right]^2 \left[ 1 - \exp\left(-2(n^2 \log n) \frac{\lambda_1}{4n^2}\right) \right]^2 = (1 - n^{-\lambda_1/2})^4 \geq 1 - 4n^{-\lambda_1/2}. \tag{A13}$$

### APPENDIX B: PROOF OF THEOREM 2

Let us look back at Protocol 2. For the process of performing the  $j$ th ( $j = 1, 2, \dots, m$ ) measurement setting on the  $K$  registers, we define the set  $\Pi^{(j)}$  to be the set which consists of these registers, and the set consisting of the remaining  $(m+1-j)K$  registers is denoted as  $\overline{\Pi}^{(j)}$ . If we set  $T = (m+2-j)K$ ,  $N = (m+1-j)K$ , and, for any  $l \in S_j$ ,

$$Y_k^l = \begin{cases} 0, & M_l^{\rho'_k} = 1 \\ 1, & M_l^{\rho'_k} = -1 \end{cases} \tag{B1}$$

in Lemma 1, where  $\rho'_k$  is the quantum state of the  $k$ th register in  $\Pi^{(j)}$  or  $\overline{\Pi}^{(j)}$  depending on  $k \in \Pi^{(j)}$  or  $k \in \overline{\Pi}^{(j)}$ , we can derive

$$\Pr\left(\sum_{k \in \overline{\Pi}^{(j)}} Y_k^l \leq \frac{(m+1-j)K}{K} \sum_{k \in \Pi^{(j)}} Y_k^l + (m+1-j)Kv\right) \geq 1 - \exp\left(-\frac{2v^2(m+1-j)KK^2}{(m+2-j)K(K+1)}\right). \tag{B2}$$

This shows that once the  $j$ th measurement setting is performed on the remaining  $(m+1-j)K$  registers, the maximal number of registers satisfying  $M_l^{\rho} = -1$  is  $(m+1-j) \sum_{k \in \Pi^{(j)}} Y_k^l + (m+1-j)Kv$  in the set  $\overline{\Pi}^{(j)}$ .

According to the above analysis, if we perform the  $j$ th measurement setting on the final  $K$  registers that are not measured, then there are at least  $K - [(m+1-j) \sum_{k \in \Pi^{(j)}} Y_k^l + (m+1-j)Kv]$  registers satisfying  $M_l^{\rho} = 1$  for any  $l \in S_j$ , i.e.,

$$\sum_{k=1}^K M_l^{\rho_k} \geq K - 2\left((m+1-j) \sum_{k \in \Pi^{(j)}} Y_k^l + (m+1-j)Kv\right). \tag{B3}$$

Utilizing Lemma 2, it follows that for any  $l \in S_j$ ,

$$\Pr\left(\frac{1}{K} \sum_{k=1}^K M_l^{\rho_k} - \frac{1}{K} \sum_{k=1}^K \overline{M_l^{\rho_k}} < t\right) \geq 1 - \exp(-Kt^2/2). \tag{B4}$$

Relations (25) and (B3) allow us to transform this into

$$\Pr\left[\text{Tr}(g_l \rho_{\text{tgt}}) > 1 - \frac{2}{K} \left((m+1-j) \sum_{k \in \Pi^{(j)}} Y_k^l + (m+1-j)Kv\right) - t\right] \geq 1 - \exp(-Kt^2/2). \tag{B5}$$

Using the estimation (10) of the fidelity in Sec. II, this yields

$$\begin{aligned}
F &\geq \frac{1}{2} - \frac{1}{2} \text{Tr}(W_4 \rho_{\text{tgt}}) = \frac{2-n}{2} + \frac{1}{2} \sum_{i=1}^n \text{Tr}(g_i \rho_{\text{tgt}}) \\
&\geq \frac{2-n}{2} + \frac{1}{2} \sum_{i=1}^n \left[ 1 - \frac{2}{K} \left( [m+1-f(i)] \sum_{k \in \Pi^{(i)}} Y_k^i + [m+1-f(i)]Kv \right) - t \right] \\
&= 1 - \sum_{i=1}^n \frac{1}{K} \left( [m+1-f(i)] \sum_{k \in \Pi^{(i)}} Y_k^i + [m+1-f(i)]Kv \right) - \frac{1}{2}nt \\
&\geq 1 - nmv - \frac{1}{2}nt - \frac{nm}{K} \max_i \sum_{k \in \Pi^{(i)}} Y_k^i,
\end{aligned} \tag{B6}$$

where the second inequality and the third inequality are obtained from Eqs. (4) and (B5), respectively. In addition, we can guarantee that Eq. (B6) holds with probability

$$\begin{aligned}
P &\geq \left\{ \prod_{i=1}^n \left[ 1 - \exp \left( -\frac{2v^2[m+1-f(i)]KK^2}{[m+2-f(i)]K(K+1)} \right) \right] \right\} \left[ 1 - \exp \left( -\frac{1}{2}Kt^2 \right) \right]^n \\
&\geq \left[ 1 - \exp \left( -\frac{1}{2}v^2K \right) \right]^n \left[ 1 - \exp \left( -\frac{1}{2}Kt^2 \right) \right]^n.
\end{aligned} \tag{B7}$$

Let us set  $v = \sqrt{\lambda_2}/n^2$  and  $t = \sqrt{\lambda_2}/n^2$ , where  $\lambda_2$  is any constant satisfying  $2 + \log_n 4 < \lambda_2 < (\frac{n-1}{1/2+m})^2$ . Combining this with the condition (26) of accepting, we conclude that the fidelity satisfies

$$F \geq 1 - \frac{1 + (1/2 + m)\sqrt{\lambda_2}}{n} \tag{B8}$$

with probability

$$P \geq \left[ 1 - \exp \left( -\frac{\lambda_2}{2n^4} n^4 \log n \right) \right]^n \left[ 1 - \exp \left( -\frac{1}{2} (n^4 \log n) \frac{\lambda_2}{n^4} \right) \right]^n = (1 - n^{-\lambda_2/2})^{2n} \geq 1 - 2n^{1-\lambda_2/2}. \tag{B9}$$

### APPENDIX C: PROOF OF THEOREM 3

Let us look back at Protocol 3. For the process of performing the  $j$ th ( $j = 1, 2, \dots, m$ ) measurement setting on the  $K$  registers, we define the set  $\Pi^{(j)}$  to be the set which consists of these registers, and the set consisting of the remaining  $(m+1-j)K$  registers is denoted as  $\overline{\Pi}^{(j)}$ . If we set  $T = (m+2-j)K$ ,  $N = (m+1-j)K$ , and

$$Y_k = \begin{cases} 0, & M_j^{\rho'_k} = 1 \\ 1, & M_j^{\rho'_k} = 0 \end{cases} \tag{C1}$$

in Lemma 1, where  $\rho'_k$  is the quantum state of the  $k$ th register in  $\Pi^{(j)}$  or  $\overline{\Pi}^{(j)}$  depending on  $k \in \Pi^{(j)}$  or  $k \in \overline{\Pi}^{(j)}$ , we can derive

$$\Pr \left( \sum_{k \in \overline{\Pi}^{(j)}} Y_k \leq \frac{(m+1-j)K}{K} \sum_{k \in \Pi^{(j)}} Y_k + (m+1-j)Kv \right) \geq 1 - \exp \left( -\frac{2v^2(m+1-j)KK^2}{(m+2-j)K(K+1)} \right). \tag{C2}$$

This suggests that once the  $j$ th measurement setting is performed on the remaining  $(m+1-j)K$  registers, the maximal number of registers satisfying  $M_j^\rho = 0$  is  $(m+1-j) \sum_{k \in \Pi^{(j)}} Y_k + (m+1-j)Kv$  in the set  $\overline{\Pi}^{(j)}$ .

According to above analysis, if we perform the  $j$ th measurement setting on the final  $K$  registers that are not measured, then there are at least  $K - [(m+1-j) \sum_{k \in \Pi^{(j)}} Y_k + (m+1-j)Kv]$  registers satisfying  $M_j^\rho = 1$ , i.e.,

$$\sum_{k=1}^K M_j^{\rho_k} \geq K - \left( (m+1-j) \sum_{k \in \Pi^{(j)}} Y_k + (m+1-j)Kv \right). \tag{C3}$$

Using Lemma 2, we get

$$\Pr \left( \frac{1}{K} \sum_{k=1}^K M_j^{\rho_k} - \frac{1}{K} \sum_{k=1}^K \overline{M_j^{\rho_k}} < t \right) \geq 1 - \exp(-2Kt^2). \tag{C4}$$

Relations (19) and (C3) allow us to transform this into

$$\Pr \left[ \text{Tr} \left( \prod_{i \in S_j} \frac{g_i + I}{2} \rho_{\text{tgt}} \right) > 1 - \frac{1}{K} \left( (m+1-j) \sum_{k \in \Pi^{(j)}} Y_k + (m+1-j)Kv \right) - t \right] \geq 1 - \exp(-2Kt^2). \quad (\text{C5})$$

Using the estimation (15) of the fidelity in Sec. II, it follows that

$$\begin{aligned} F &\geq 1 - \frac{1}{2} [\text{Tr}(W_3 \rho_{\text{tgt}}) - (3-2m)] = 1 - \frac{1}{2} \left( \text{Tr} \left\{ \left[ 3I - 2 \sum_{j=1}^m \left( \prod_{i \in S_j} \frac{g_i + I}{2} \right) \right] \rho_{\text{tgt}} \right\} - (3-2m) \right) \\ &\geq 1 - \sum_{j=1}^m \frac{1}{K} \left( (m+1-j) \sum_{k \in \Pi^{(j)}} Y_k + (m+1-j)Kv \right) - mt \geq 1 - m^2 v - mt - \frac{m}{K} \sum_{j=1}^m \sum_{k \in \Pi^{(j)}} Y_k, \end{aligned} \quad (\text{C6})$$

where the equality and the second inequality are obtained from Eqs. (3) and (C5), respectively. In addition, we can guarantee that Eq. (C6) holds with probability

$$\begin{aligned} P &\geq \left\{ \prod_{j=1}^m \left[ 1 - \exp \left( -\frac{2v^2(m+1-j)KK^2}{(m+2-j)K(K+1)} \right) \right] \right\} [1 - \exp(-2Kt^2)]^m \\ &\geq \left[ 1 - \exp \left( -\frac{1}{2} v^2 K \right) \right]^m [1 - \exp(-2Kt^2)]^m. \end{aligned} \quad (\text{C7})$$

Let us set  $v = \sqrt{\lambda_3}/(2mn)$  and  $t = \sqrt{\lambda_3}/(4mn)$ , where  $\lambda_3$  is any constant satisfying  $2 \log_n 2m < \lambda_3 < (\frac{n-1}{m/2+1/4})^2$ . Combining this with the condition (30) of accepting, we conclude that the fidelity satisfies

$$F \geq 1 - \frac{1 + (m/2 + 1/4)\sqrt{\lambda_3}}{n} \quad (\text{C8})$$

with probability

$$P \geq \left[ 1 - \exp \left( -\frac{1}{2} \frac{\lambda_3}{4m^2 n^2} 4m^2 n^2 \log n \right) \right]^m \left[ 1 - \exp \left( -2(4m^2 n^2 \log n) \frac{\lambda_3}{16m^2 n^2} \right) \right]^m = (1 - n^{-\lambda_3/2})^{2m} \geq 1 - 2mn^{-\lambda_3/2}. \quad (\text{C9})$$

---

[1] F. Arute *et al.*, *Nature (London)* **574**, 505 (2019).  
 [2] P. W. Shor, in *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 1994), p. 124.  
 [3] J. Preskill, *Quantum* **2**, 79 (2018).  
 [4] A. Childs, *Quantum Inf. Comput.* **5**, 456 (2005).  
 [5] A. Broadbent, J. F. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 2009), p. 517.  
 [6] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, *Science* **335**, 303 (2012).  
 [7] T. Morimae and K. Fujii, *Nat. Commun.* **3**, 1036 (2012).  
 [8] T. Morimae, *Phys. Rev. Lett.* **109**, 230502 (2012).  
 [9] V. Dunjko, E. Kashefi, and A. Leverrier, *Phys. Rev. Lett.* **108**, 200502 (2012).  
 [10] T. Morimae and K. Fujii, *Phys. Rev. A* **87**, 050301(R) (2013).  
 [11] T. Morimae and K. Fujii, *Phys. Rev. Lett.* **111**, 020502 (2013).  
 [12] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, *Phys. Rev. Lett.* **111**, 230501 (2013).  
 [13] Q. Li, W. H. Chan, C. Wu, and Z. Wen, *Phys. Rev. A* **89**, 040302(R) (2014).  
 [14] Y. B. Sheng and L. Zhou, *Sci. Rep.* **5**, 7815 (2015).  
 [15] T. Morimae, V. Dunjko, and E. Kashefi, *Quantum Inf. Comput.* **15**, 200 (2015).  
 [16] C. A. Pérez-Delgado and J. F. Fitzsimons, *Phys. Rev. Lett.* **114**, 220502 (2015).  
 [17] Y. Takeuchi, K. Fujii, R. Ikuta, T. Yamamoto, and N. Imoto, *Phys. Rev. A* **93**, 052307 (2016).  
 [18] X. Tan and X. Zhou, *Ann. Telecommun.* **72**, 589 (2017).  
 [19] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).  
 [20] R. Raussendorf, J. Harrington, and K. Goyal, *Ann. Phys. (NY)* **321**, 2242 (2006).  
 [21] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, *Nat. Phys.* **5**, 19 (2009).  
 [22] B. W. Reichardt, F. Unger, and U. Vazirani, *Nature (London)* **496**, 456 (2013).  
 [23] T. Morimae, *Phys. Rev. A* **89**, 060302(R) (2014).  
 [24] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, *arXiv:1502.02563*.  
 [25] M. Hayashi and T. Morimae, *Phys. Rev. Lett.* **115**, 220502 (2015).  
 [26] A. Gheorghiu, E. Kashefi, and P. Wallden, *New J. Phys.* **17**, 083040 (2015).  
 [27] M. McKague, *Theory Comput.* **12**, 1 (2016).

- [28] J. F. Fitzsimons and E. Kashefi, *Phys. Rev. A* **96**, 012303 (2017).
- [29] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, [arXiv:1704.04487](https://arxiv.org/abs/1704.04487).
- [30] A. Gheorghiu, P. Wallden, and E. Kashefi, *New J. Phys.* **19**, 023043 (2017).
- [31] K. Fujii and M. Hayashi, *Phys. Rev. A* **96**, 030301(R) (2017).
- [32] M. Hayashi and M. Hajdušek, *Phys. Rev. A* **97**, 052308 (2018).
- [33] J. F. Fitzsimons, M. Hajdušek, and T. Morimae, *Phys. Rev. Lett.* **120**, 040501 (2018).
- [34] Y. Takeuchi and T. Morimae, *Phys. Rev. X* **8**, 021060 (2018).
- [35] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, *Theory Comput. Syst.* **63**, 715 (2019).
- [36] Y. Takeuchi, T. Morimae, A. Mizutani, and J. F. Fitzsimons, *npj Quantum Inf.* **5**, 27 (2019).
- [37] N. Liu, T. F. Demarie, S.-H. Tan, L. Aolita, and J. F. Fitzsimons, *Phys. Rev. A* **100**, 062309 (2019).
- [38] A. Coladangelo, A. B. Grilo, S. Jeffery, and T. Vidick, *Adv. Crypt.* **11478**, 247 (2019).
- [39] Q. Xu, X. Tan, and R. Huang, *Entropy* **22**, 996 (2020).
- [40] M. Hein, J. Eisert, and H. J. Briegel, *Phys. Rev. A* **69**, 062311 (2004).
- [41] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Lett. A* **223**, 1 (1996).
- [42] B. M. Terhal, *Phys. Lett. A* **271**, 319 (2000).
- [43] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, *Phys. Rev. A* **62**, 052310 (2000).
- [44] O. Gühne and G. Tóth, *Phys. Rep.* **474**, 1 (2009).
- [45] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Rev. Mod. Phys.* **81**, 865 (2009).
- [46] D. Chruściński and G. Sarbicki, *J. Phys. A* **47**, 483001 (2014).
- [47] M. Curty, M. Lewenstein, and N. Lütkenhaus, *Phys. Rev. Lett.* **92**, 217903 (2004).
- [48] S. Popescu and D. Rohrlich, *Found. Phys.* **24**, 379 (1994).
- [49] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera, *Phys. Rev. Lett.* **92**, 087902 (2004).
- [50] G. Tóth and O. Gühne, *Phys. Rev. Lett.* **94**, 060501 (2005).
- [51] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe, *Nature (London)* **404**, 256 (2000).
- [52] R. Raussendorf, J. Harrington, and K. Goyal, *New J. Phys.* **9**, 199 (2007).
- [53] G. Tóth and O. Gühne, *Phys. Rev. A* **72**, 022340 (2005).
- [54] M. Mhalla and S. Perdrix, [arXiv:1202.6551](https://arxiv.org/abs/1202.6551).
- [55] O. Gühne, M. Reimpell, and R. F. Werner, *Phys. Rev. Lett.* **98**, 110502 (2007).
- [56] R. T. Rockafellar, *Convex Analysis* (Princeton University Press, Princeton, NJ, 1997).
- [57] R. J. Serfling, *Ann. Stat.* **2**, 39 (1974).
- [58] W. Hoeffding, *J. Am. Stat. Assoc.* **58**, 13 (1963).
- [59] R. Raussendorf, D. E. Browne, and H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
- [60] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, *New J. Phys.* **15**, 113022 (2013).
- [61] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, *Phys. Rev. A* **79**, 062318 (2009).