Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing

Article *in* Physical Review Letters · May 2015

DOI: 10.1103/PhysRevLett.115.220502 · Source: arXiv

2 authors, including:

Masahito Hayashi
Nagoya University
304 PUBLICATIONS **4,372** CITATIONS

SEE PROFILE

Verifiable measurement-only blind quantum computing with stabilizer testing

Masahito Hayashi[1,2] and Tomoyuki Morimae[3]

[1] *Graduate School of Mathematics, Nagoya University, Furocho, Chikusa-ku, Nagoya, 464-860, Japan*
[2] *Centre for Quantum Technologies, National University of Singapore, 117543, Singapore*
[3] *ASRLD Unit, Gunma University, 1-5-1 Tenjincho, Kiryu-shi, Gunma, 376-0052, Japan*

(Dated: November 30, 2015)

We introduce a simple protocol for verifiable measurement-only blind quantum computing. Alice, a client, can perform only single-qubit measurements, whereas Bob, a server, can generate and store entangled many-qubit states. Bob generates copies of a graph state, which is a universal resource state for measurement-based quantum computing, and sends Alice each qubit of them one by one. Alice adaptively measures each qubit according to her program. If Bob is honest, he generates the correct graph state, and therefore Alice can obtain the correct computation result. Regarding the security, whatever Bob does, Bob cannot learn any information about Alice's computation because of the no-signaling principle. Furthermore, malicious Bob does not necessarily send the copies of the correct graph state, but Alice can check the correctness of Bob's state by directly verifying stabilizers of some copies.

Blind quantum computing is a quantum cryptographic protocol that enables Alice (a client), who does not have any sophisticated quantum technology, to delegate her quantum computing to Bob (a server), who has a sufficiently powerful quantum computer, without leaking any her privacy. The first protocol of blind quantum computing that uses the measurement-based quantum computing [1] was proposed by Broadbent, Fitzsimons, and Kashefi [2], and a proof-of-principle experiment was demonstrated with photonic qubits [3]. In the protocol of Ref. [2], Alice generates many randomly-rotated single-qubit states, and sends them to Bob. Bob generates a universal resource state of the measurement-based quantum computing by applying entangling gates on qubits sent from Alice. Then, they do two-way classical communications: Alice instructs Bob how to measure each qubit, and Bob returns measurement results so that Alice can perform the feed-forward calculations. It was shown in Ref. [2] that if Bob is honest, Alice can obtain the correct quantum computing result (which we call the correctness), and that whatever evil Bob does, he cannot learn anything about Alice's input, output, and program (which we call the blindness) [4]. (See also Ref. [5] for a precise proof of the security.) Inspired by the seminal result, plenty of improvements have been done [6–20]. For example, it was shown that instead of single-qubit states generation, single-qubit measurements [6] or coherent states generation [7] are sufficient for Alice. In the protocol of Ref. [6], so called the measurement-only blind quantum computing, Bob generates a universal resource state of measurement-based quantum computing (Fig 1(a)), and sends each qubit of the resource state one by one to Alice (Fig. 1(b)). Alice adaptively measures each qubit according to her program (Fig. 1(b)). Since adaptive single-qubit measurements on certain states are universal [1, 21–23], Alice with only single-qubit measurements ability can perform universal quantum computing if Bob prepares the correct resource state. Furthermore, since this protocol is a one-way quantum communication from Bob to Alice, the blindness is guaranteed by the no-signaling principle [6]. Here, the no-signaling principle is one of the most fundamental assumptions in physics, which says that if Alice and Bob share a system she cannot transmit any her message to Bob whatever they do on their systems. Quantum physics respects the no-signaling principle.

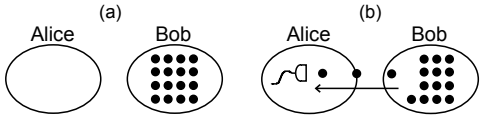

FIG. 1: The measurement-only blind quantum computing. (a) Bob generates a resource state. (b) Bob sends Alice each qubit of the resource state one by one. Alice adaptively measures each qubit.

In addition to the correctness and the blindness, the verifiability is another important requirement for blind quantum computing. The verifiability means that Alice can check the correctness of Bob's computation. Although the blindness guarantees that Alice's privacy is kept secret against malicious Bob, it does not guarantee the correctness of the computation result with malicious Bob: Bob cannot learn Alice's secret, but he can mess up the computation. In order to avoid being palmed off a wrong result, Alice needs some statistical test to verify the correctness of Bob's computing. There are several protocols that enable verifiable blind quantum computing [8–11, 24, 25]. Some of them [9, 24, 25] elegantly achieve the completely classical client, but a trade-off is the requirement of more than two servers who do not communicate with each other. Although pursuing the completely classical client is an important direction, in particular, for the goal of constructing an interactive proof of BQP, where the assumption of non-communicating multi provers is natural, in this paper we restrict ourselves to the single-server setup assuming some minimum quantum technologies for the client, since in the context of blind quantum computing, as-

suming some minimum quantum technologies for the client is more realistic than to assume that the client can verify that remote servers are not communicating with each other. These results also achieve the device independence. Although our protocol assumes the correctness of measurement devices, it enables to derive a more practical bound suitable for experiments. Protocols in Refs. [8, 10, 11] need only a single server by assuming some minimum quantum technologies, which are available in today's laboratories, for the client. (The protocol of Ref. [10] requires single-qubit states generations, and those of Refs. [8, 11] require single-qubit measurements for the client.) The idea of the verification in the protocols of Refs. [8–11] is to use trap qubits: Alice secretly hides trap qubits in the resource state, and any disturbance of a trap signals Bob's dishonesty [8–11]. An experimental demonstration of the idea was done with photonic qubits [26].

In this paper, we propose another protocol for verifiable measurement-only blind quantum computing. The blindness is again guaranteed by the no-signaling principle like Ref. [6]. The verifiability is, on the other hand, achieved in a more straightforward way: instead of hiding traps, Alice directly checks whether the state sent from Bob is correct or not by testing stabilizers [27]. Alice asks Bob to generate $2k+1$ copies $|G\rangle^{\otimes 2k+1}$ of the graph state $|G\rangle$, where $|G\rangle$ is an n-qubit graph state and $k = poly(n)$. The graph state $|G\rangle$ is defined by $|G\rangle \equiv \left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes n}$, where $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, E is the set of edges of G, and CZ_e is the Controlled-Z gate, $CZ \equiv |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes Z$, acting on the pair of vertices sharing the edge e. The graph state $|G\rangle$ has the stabilizers $X_j \bigotimes_{i\in N(j)} Z_i$, for $j = 1, 2, ..., n$, where $N(j)$ is the set of the vertices connected to j. Alice uses randomly chosen $2k$ copies of $|G\rangle^{\otimes 2k+1}$ to check stabilizers, and the rest of it for her computation. If Bob is honest, he generates $|G\rangle^{\otimes 2k+1}$, and in this case we will show that she passes the test with probability 1. If Bob is evil, on the other hand, he might generate another $n(2k+1)$-qubit state. However, we will show that if she passes the test, the closeness of the single copy to the correct graph state $|G\rangle$ is guaranteed with a sufficiently small significance level. Any graph state can be used for our protocol as long as the corresponding graph G is bipartite. Therefore, for example, Alice can perform the fault-tolerant topological measurement-based quantum computing [21] by taking $|G\rangle$ as the Raussendorf-Harrington-Goyal lattice [21] (Fig. 2(a)).

Note that there are several proposals for testing quantum gate operations [30, 31], but testing quantum circuit models assumes the identical and independent properties of each gate, and suffers from the scalability and complexity of the analysis. On the other hand, our result in the present paper (and Ref. [25]) demonstrate that testing quantum computing becomes much easier if we consider a measurement-based quantum computing model, which is a new interesting advantage of the measurement-based quantum computing model over the circuit model. For more details about the relations between our result and previous works, see Appendix.

Protocol.— Our protocol runs as follows:

1. Honest Bob generates $|G\rangle^{\otimes 2k+1}$, where $|G\rangle$ is an n-qubit graph state on a bipartite graph G, whose vertices are divided into two disjoint sets W and B. (Fig. 2(a) and (b).) Bob sends each qubit of it one by one to Alice. Evil Bob can generate any $n(2k+1)$-qubit state ρ instead of $|G\rangle^{\otimes 2k+1}$.

2. Alice divides $2k+1$ blocks of n qubits into three groups by random choice. (Fig. 2(c).) The first group consists of k blocks of n qubits. The second group consists of k blocks of n qubits. The third group consists of a single block of n qubits.

3. Alice uses the third group for her computation. Other blocks are used for the test, which will be explained later. (Fig. 2(c).)

4. If Alice passes the test, she accepts the result of the computation performed on the third group.

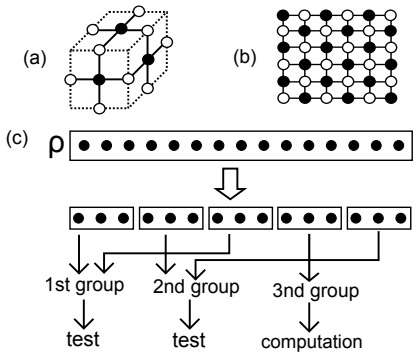

FIG. 2: (a) The RHG lattice. (b) An example of bipartite graphs: the two-dimensional square lattice. Black and white colors indicate the bipartitions B and W, respectively. (c) An example for $n = 3$, $k = 2$. Two blocks go to the first group and the other two blocks go to the second group. The left block goes to the third group.

For each block of the first and second groups, Alice performs the following test:

1. For each block of the first group, Alice measures qubits of W in the Z basis and qubits of B in the X basis. (Fig. 3(a).)

2. For each block of the second group, Alice measures qubits of B in the Z basis and qubits of W in the X basis. (Fig. 3(b).)

3. If the measurement outcomes in the X basis coincide with the values predicted from the outcomes in the Z basis (in terms of the stabilizer relations),

then the test is passed. If any outcome in the X basis that violates the stabilizer relations is obtained, Alice rejects.

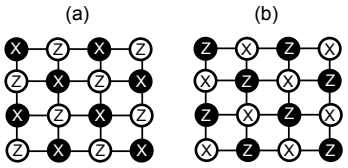

FIG. 3: An example for the two-dimensional square lattice. The measurement pattern for the first group (a) and the second group (b).

Analysis.— Let us analyze the correctness, blindness, and verifiability of our protocol. First, our protocol is a one-way quantum communication from Bob to Alice, and therefore, the blindness is guaranteed by the no-signaling principle as in the protocol of Ref. [6]. Second, it is obvious that if $\rho = |G\rangle\langle G|^{\otimes 2k+1}$, then Alice passes the test with probability 1. Therefore, if Bob is honest, Alice passes the test with probability 1 and she obtains the correct computation result on the third group. Hence the correctness is satisfied. Finally, to study the verifiability, we consider the following theorem:

Theorem 1 *Assume that $\alpha > \frac{1}{2k+1}$. If the test is passed, with significance level α, we can guarantee that the resultant state σ of the third group satisfies*

$$\langle G|\sigma|G\rangle \geq 1 - \frac{1}{\alpha(2k+1)}. \tag{1}$$

(Note that the significance level is the maximum passing probability when malicious Bob sends incorrect states so that the resultant state σ does not satisfy (1) [28].) The proof of the theorem is given below and in Appendix. From the theorem and the relation between the fidelity and trace norm [32, (6.106)], we can conclude the verifiability: If Alice passes the test, she can guarantee

$$\Big|\mathrm{Tr}(C\sigma) - \mathrm{Tr}(C|G\rangle\langle G|)\Big| \leq \frac{1}{\sqrt{\alpha(2k+1)}}$$

for any POVM C with the significance level α. If we take $\alpha = \frac{1}{\sqrt{2k+1}}$, for example, the left-hand side of the above inequality is $\frac{1}{(2k+1)^{1/4}} \to 0$ if $k \to \infty$, and therefore the verifiability is satisfied. Note that the lower bound, $\alpha > \frac{1}{2k+1}$, of the significance level α is tight, since if Bob generates $2k$ copies of the correct state $|G\rangle$ and a single copy of a wrong state, Bob can fool Alice with probability $\frac{1}{2k+1}$, which corresponds to $\alpha = \frac{1}{2k+1}$.

Proof of Theorem.— The proof of the theorem is based on several interesting insights:

1. By considering an appropriate subspace, we can reduce the problem to the test of a maximally-entangled state.

2. For the test of a maximally-entangled state, verifications of coincidences of X measurement results with Z measurement results are sufficient. Furthermore, since we are interested in the fidelity between the given state and a maximally-entangled state, we can consider, without loss of generality, the discretely twirled version of the given state, which drastically simplifies the problem [29].

3. Finally, since we check the coincidence or discrepancy of the measurement results between two parties of the given bipartite cut, we have only to consider a distribution on $(0,0)$, $(0,1)$, $(1,0)$, and $(1,1)$ for each block, and therefore we can reduce the problem to a classical hypothesis testing.

Let us explain the first point. Employing suitable classical data conversions, we can assume the following. The systems $\mathcal{H}_B$ and $\mathcal{H}_W$ are written as $\mathcal{K}_B \otimes \mathcal{K}'_B$ and $\mathcal{K}_W \otimes \mathcal{K}'_W$ by using an n'_B-qubit system $\mathcal{K}_B$ and an n'_W-qubit system $\mathcal{K}_W$, respectively. We denote the eigenstate corresponding to the eigenvalue all 0 of X's in $\mathcal{K}'_B$ by $|+\rangle_{B'}$, which is the graph state with isolated sites with no edge. Similarly, we define $|+\rangle_{W'}$. So, we find that the systems $\mathcal{K}_B$ and $\mathcal{K}_W$ are the same dimension, i.e., $n'_B = n'_W$. Let $|G'\rangle$ be the graph state on $\mathcal{K}_B \otimes \mathcal{K}_W$ whose graph is composed of isolated edges. The true state is given as the state $|G'\rangle \otimes |+\rangle_{B'} \otimes |+\rangle_{W'}$. In this way, we can reduce the problem to that of the maximally-entangled state. Note that Alice's measurements on $\mathcal{H}_B$ and $\mathcal{H}_W$ are replaced by on $\mathcal{K}_B$ and $\mathcal{K}_W$, respectively. Applying the original Alice's measurement, Alice can realize the above modified measurement. The detail of this discussion is given in Appendix.

Now let us explain the second point. We focus on the Hilbert space $(\mathcal{K}_B \otimes \mathcal{K}_W)^{\otimes(2k+1)}$. Since the three groups are randomly chosen, the state ρ is permutation invariant. Let us denote elements of $\mathbb{F}_2^{n'_B}$ by $x = (x_1, \ldots, x_{n'_B})$, etc. We define operators $\mathsf{X}^x \equiv X^{x_1} \otimes \cdots \otimes X^{x_{n'_B}}$, $\mathsf{Z}^z \equiv Z^{z_1} \otimes \cdots \otimes Z^{z_{n'_B}}$, on $(\mathbb{C}^2)^{\otimes n'_B}$, which satisfy

$$\mathsf{X}^x_B \otimes \mathsf{Z}^{-x}_W |G'\rangle = |G'\rangle, \quad \mathsf{X}^x_W \otimes \mathsf{Z}^{-x}_B |G'\rangle = |G'\rangle. \tag{2}$$

In the following, we regard X^x_B, Z^z_B as operators on $\mathcal{K}_B$ and X^x_W, Z^z_W as operators on $\mathcal{K}_W$. Here, we distinguish x and $-x$ so that we can easily extend our analysis to the qudit case.

Furthermore, for $\mathbf{x} = (x^1, \ldots, x^{2k+1}) \in (\mathbb{F}_2^{n'_B})^{2k+1}$ and $\mathbf{z} = (z^1, \ldots, z^{2k+1}) \in (\mathbb{F}_2^{n'_B})^{2k+1}$, using the operator $\mathsf{W}_B^{x,z} \equiv \mathsf{X}^x_B \mathsf{Z}^z_B$ on $\mathcal{K}_B$, we define $\mathsf{W}_B^{\mathbf{x},\mathbf{z}} \equiv \mathsf{W}_B^{x^1,z^1} \otimes \cdots \otimes \mathsf{W}_B^{x^{2k+1},z^{2k+1}}$ on $\mathcal{K}_B^{\otimes 2k+1}$. Also, we define $\mathsf{W}_W^{x,z}$ on $\mathcal{K}_W$, and $\mathsf{W}_W^{\mathbf{x},\mathbf{z}}$ on $\mathcal{K}_W^{\otimes 2k+1}$, in the same way. Eq. (2) implies that $\mathsf{W}_B^{\mathbf{x},\mathbf{z}} \otimes \mathsf{W}_W^{-\mathbf{z},-\mathbf{x}} |G'\rangle^{\otimes 2k+1} = |G'\rangle^{\otimes 2k+1}$. Hence,

$$\begin{aligned} &\mathrm{Tr}\left[(\mathsf{W}_B^{\mathbf{x},\mathbf{z}} \otimes \mathsf{W}_W^{-\mathbf{z},-\mathbf{x}})^\dagger \rho (\mathsf{W}_B^{\mathbf{x},\mathbf{z}} \otimes \mathsf{W}_W^{-\mathbf{z},-\mathbf{x}}) |G'\rangle\langle G'|^{\otimes 2k+1}\right] \\ =\ &\mathrm{Tr}\left(\rho |G'\rangle\langle G'|^{\otimes 2k+1}\right). \end{aligned}$$

Thus, the discrete-twirled state

$$\overline{\rho} \equiv \sum_{\mathbf{x},\mathbf{z}} 2^{-2n'_B(2k+1)} (\mathsf{W}_B^{\mathbf{x},\mathbf{z}} \otimes \mathsf{W}_W^{-\mathbf{z},-\mathbf{x}})^\dagger \rho (\mathsf{W}_B^{\mathbf{x},\mathbf{z}} \otimes \mathsf{W}_W^{-\mathbf{z},-\mathbf{x}})$$

satisfies $\mathrm{Tr}\,(\overline{\rho}|G'\rangle\langle G'|^{\otimes 2k+1}) = \mathrm{Tr}\,(\rho|G'\rangle\langle G'|^{\otimes 2k+1})$ [29]. Also, we have

$$\begin{aligned}
\mathrm{Tr}_1\Big[(\mathrm{Tr}_{2,3}\overline{\rho})|G'\rangle\langle G'|^{\otimes k}\Big] &= \mathrm{Tr}_1\Big[(\mathrm{Tr}_{2,3}\rho)|G'\rangle\langle G'|^{\otimes k}\Big], \\
\mathrm{Tr}_2\Big[(\mathrm{Tr}_{1,3}\overline{\rho})|G'\rangle\langle G'|^{\otimes k}\Big] &= \mathrm{Tr}_2\Big[(\mathrm{Tr}_{1,3}\rho)|G'\rangle\langle G'|^{\otimes k}\Big], \\
\mathrm{Tr}_3\Big[(\mathrm{Tr}_{1,2}\overline{\rho})|G'\rangle\langle G'|\Big] &= \mathrm{Tr}_3\Big[(\mathrm{Tr}_{1,2}\rho)|G'\rangle\langle G'|\Big].
\end{aligned}$$

Therefore, we have only to consider the discretely twirled version of ρ. Note that the upper subscript of x and z expresses the choice of group, and the lower subscript of x and z expresses the site of the modified graph.

Finally, let us explain the third point. Since $(\mathsf{W}_B^{\mathbf{x},\mathbf{z}} \otimes \mathsf{W}_W^{-\mathbf{z},-\mathbf{x}})\overline{\rho}(\mathsf{W}_B^{\mathbf{x},\mathbf{z}} \otimes \mathsf{W}_W^{-\mathbf{z},-\mathbf{x}})^\dagger = \overline{\rho}$ and ρ is permutation-invariant, the state $\overline{\rho}$ is written with a permutation-invariant distribution P on $\mathbb{F}_2^{2n'_B(2k+1)}$ as [29]

$$\overline{\rho} = \sum_{\mathbf{x},\mathbf{z}} P(\mathbf{x},\mathbf{z}) \mathsf{W}_B^{\mathbf{x},\mathbf{z}} |G'^{\otimes 2k+1}\rangle\langle G'^{\otimes 2k+1}| (\mathsf{W}_B^{\mathbf{x},\mathbf{z}})^\dagger.$$

Then, we define the function f from $(\mathbb{F}_2^{n'_B})^{2(2k+1)}$ to $(\{0,1\}^2)^{(2k+1)}$ as $f : (\mathbf{x},\mathbf{z}) \mapsto (s_1,t_1),\ldots,(s_{2k+1},t_{2k+1})$, where $s_i := \begin{cases} 0 & \text{if } x^i = 0 \\ 1 & \text{if } x^i \neq 0 \end{cases}$ and $t_i := \begin{cases} 0 & \text{if } z^i = 0 \\ 1 & \text{if } z^i \neq 0. \end{cases}$

Here, x^i and z^i are elements of $\mathbb{F}_2^{n'_B}$. So, 0 in the above conditions expresses the zero vector in $\mathbb{F}_2^{n'_B}$ although s_i is an element of $\mathbb{F}_2$.

We introduce the distributions $\hat{P}((s_1,t_1),\ldots,(s_{2k+1},t_{2k+1}))$ on $(\{0,1\}^2)^{(2k+1)}$ as $\hat{P} := P \circ f^{-1}$.

Once, Bob's operation is given, the values $s_1,\ldots,s_{2k+1}$, $t_1,\ldots,t_{2k+1}$ are given as random variables although half of $s_1,\ldots,s_{2k}$, $t_1,\ldots,t_{2k}$ can be observed. To employ the notations of probability theory, we express them using the capital letters as $S_1,\ldots,S_{2k+1}$, $T_1,\ldots,T_{2k+1}$. Hence, $\hat{P}(S_i = 0)$ expresses the probability that the i-th measurement outcome of X basis of B system coincides with the prediction by the i-th measurement outcome of Z basis of W system. So, to show Theorem 1, it is enough to show the following theorem. Similarly, $\hat{P}(T_{k+i} = 0)$ expresses the probability that the $k+i$-th measurement outcome of X basis of W system coincides with the prediction by the $k+i$-th measurement outcome of Z basis of B system. So, to show Theorem 1, it is enough to show the following theorem.

Theorem 2 *Assume that $\alpha > \frac{1}{2k+1}$. When the distribution $\hat{P}$ satisfies*

$$\begin{aligned}
&\hat{P}(S_{2k+1} = T_{2k+1} = 0 | S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k) \\
\ge\ & 1 - \frac{1}{\alpha(2k+1)},
\end{aligned}$$

the probability $\hat{P}(S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k)$ is upper bounded by α.

In this way, we have reduced the problem to the classical hypothesis testing. The proof of Theorem 2 is given in Appendix.

Acknowledgments

MH is partially supported by the JSPS Grant-in-Aid for Scientific Research (A) No. 23246071 and the National Institute of Information and Communication Technology (NICT), Japan. The Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme. TM is supported by the JSPS Grant-in-Aid for Young Scientists (B) No.26730003 and the MEXT JSPS Grant-in-Aid for Scientific Research on Innovative Areas No.15H00850.

Appendix A: Relation to previous works

Here we discuss relations between our result and previous works. The hypothesis testing of an entangled state by local measurements was initiated by the paper [33]. The paper [33] treats only the maximally entangled state. The next paper [34] derived its asymptotic optimal performance in the i.i.d. setting. Then, the papers [35–38] extended these results to the case of a non-maximally entangled state. However, these papers consider only the locality condition between two parties. To apply the hypothesis testing to the blind quantum computation based on the measurement based quantum computation, we need the following conditions.

(1) The test can be applied to the case of a graph state.

(2) Our quantum operations are restricted to single-qubit measurements.

Since the previous studies [33–38] do not satisfy both conditions, we cannot use them. The papers [39, 40] satisfy these conditions as the verification of graph states, but their results assume i.i.d. samples, which is somehow reasonable in laboratory experiments, but cannot be accepted in quantum cryptography where a malicious adversary can do anything. That is, we need the following additional requirement.

(3) We cannot assume i.i.d. samples.

Therefore, these results cannot be directly used for the verification in blind quantum computing. Our protocol satisfies all of these conditions.

The verification in blind quantum computing was initiated in Ref. [10]. The idea of their protocol is to use the trap technique: Alice secretly hides isolated qubits

as traps, and if a trap is changed by Bob, she can detect his malicious behavior. Several generalizations of Ref. [10] have been obtained [11, 41, 42], but all of them essentially use the same idea, namely, the trap technique. Our protocol, on the other hand, uses a completely different technique for the verification, i.e., the direct graph state testing, for the first time.

The graph state verification is also used in the context of the multiprover interactive proof system. For example, Ref. [25] gave an elegant protocol that uses a device-independent graph state verification. However, the results in multiprover interactive proof system can neither be directly used in blind quantum computing, since the assumption that provers do not communicate with each other is not natural in the blind quantum computing.

Appendix B: Analysis of local conversion for a bipartite graph state

We show how the graph state $|G\rangle$ is converted to $|G'\rangle \otimes |+\rangle_{B'} \otimes |+\rangle_{W'}$. For this purpose, we define the notations more formally. When the true state is $|G\rangle$, the outcome of measurement with X basis in the party B takes values in the subspace over the finite filed $\mathbb{F}_2$. We denote the subspace by V_B, and denote its dimension by n'_B. The orthogonal complement is denoted by V'_B. Then, the space of the measurement outcome with X basis in the party B is written as $V_B \oplus V'_B$. So, we denote the Hilbert space corresponding to V_B and V'_B by $\mathcal{K}_B$ and $\mathcal{K}'_B$, respectively. Then, we have $\mathcal{H}_B = \mathcal{K}_B \otimes \mathcal{K}'_B$. We denote the eigenstate corresponding to the eigenvalue all 0 of X's in $\mathcal{K}'_B$ by $|+\rangle_{B'}$, which is the graph state with isolated sites with no edge. Similarly, we define V_W, V'_W, $\mathcal{K}_W$, $\mathcal{K}'_W$, n'_W and $|+\rangle_{W'}$ and have $\mathcal{H}_W = \mathcal{K}_W \otimes \mathcal{K}'_W$ and $n'_W = n'_B$. Then, we define the graph state $|G'\rangle$ on $\mathcal{K}_B \otimes \mathcal{K}_W$ whose graph is composed of isolated edges. In the following, we show that the true state is given as the state $|G'\rangle \otimes |+\rangle_{B'} \otimes |+\rangle_{W'}$.

For an invertible $n_B \times n_B$ matrix C, we define the unitary operator $U_{C,Z,B}$ as

$$U_{C,Z,B} := \sum_{z \in \mathbb{F}_2^{n_B}} |Cz\rangle_B \ {}_B\langle z|.$$

Using the X basis states $|x\rangle_{X,B}$, we define the unitary operator $U_{C,X,B}$ as

$$U_{C,X,B} := \sum_{x \in \mathbb{F}_2^{n_B}} |Cx\rangle_{X,B} \ {}_{X,B}\langle x|.$$

Then, we have the relation

$$U_{C,X,B} = U_{(C^{-1})^T,Z,B},$$

which can be shown as follows.

$$\begin{aligned}
&U_{C,X,B}|z\rangle_B \\
=&\frac{1}{2^{n_B/2}} \sum_{x \in \mathbb{F}_2^{n_B}} |Cx\rangle_{X,B} \ {}_{X,B}\langle x| \sum_{x' \in \mathbb{F}_2^{n_B}} (-1)^{x' \cdot z} |x\rangle_B \\
=&\frac{1}{2^{n_B/2}} \sum_{x \in \mathbb{F}_2^{n_B}} (-1)^{x \cdot z} |Cx\rangle_{X,B} \\
=&\frac{1}{2^{n_B/2}} \sum_{x' \in \mathbb{F}_2^{n_B}} (-1)^{C^{-1}x' \cdot z} |x'\rangle_{X,B} = |(C^{-1})^T z\rangle_B.
\end{aligned}$$

Similarly, we can define $U_{D,X,W}$ and $U_{D,X,W}$ for an invertible $n_W \times n_W$ matrix D.

Next, given the graph state $|G\rangle$, we define the $n_B \times n_W$ matrix $A = (a_{i,j})$ as follows. When the site j of W is connected to the site i of B, $a_{i,j}$ is 1. Otherwise, $a_{i,j}$ is zero. Then, we have

$$|G\rangle = \frac{1}{2^{n_W/2}} \sum_{z \in \mathbb{F}_2^{n_W}} |Az\rangle_{X,B} |z\rangle_W.$$

Then, when we measure W with the Z basis and obtain the outcome z, we obtain Az with the X measurement on B. Then, we have

$$|G\rangle = \frac{1}{2^{n_B/2}} \sum_{z \in \mathbb{F}_2^{n_B}} |z\rangle_{X,B} |A^T z\rangle_W$$

because any vector $z' \in \mathbb{F}_2^{n_B}$ satisfies

$$\begin{aligned}
&{}_B\langle z'|G\rangle \\
=&\frac{1}{2^{n_B/2}} \sum_{x \in \mathbb{F}_2^{n_B}} {}_{X,B}\langle x|(-1)^{x \cdot z'} \frac{1}{2^{n_W/2}} \sum_{z \in \mathbb{F}_2^{n_W}} |Az\rangle_{X,B} |z\rangle_W \\
=&\frac{1}{2^{n_B/2}} (-1)^{Az \cdot z'} \frac{1}{2^{n_W/2}} \sum_{z \in \mathbb{F}_2^{n_W}} |z\rangle_W \\
=&\frac{1}{2^{n_B/2}} |A^T z'\rangle_{X,W}.
\end{aligned}$$

Now, we choose a basis $c_1, \ldots, c_{n'_B}$ of the n'_B-dimensional subspace V_B that is composed of the possible outcomes with X basis in B. Also, we choose $n_B - n'_B$ vectors $c_{n'_B+1}, \ldots, c_{n_B}$ of $\mathbb{F}_2^{n_B}$ such that $c_1, \ldots, c_{n_B}$ form a basis of $\mathbb{F}_2^{n_B}$. We choose n'_W vectors $d_1, \ldots, d_{n'_W}$ of $\mathbb{F}_2^{n_W}$ such that $c_i = Ad_i$, and choose a basis $d_{n'_W+1}, \ldots, d_{n_W}$ of the kernel of A. Then, we define the invertible $n_B \times n_B$ matrix C and the invertible $n_W \times n_W$ matrix D by

$$\begin{aligned}
C &= (c_1 \ldots c_{n_B}) \\
D &= (d_1 \ldots d_{n_W}).
\end{aligned}$$

So, we define the $n_B \times n_W$ matrix $A' := C^{-1}AD$, which is written as

$$A' = \begin{pmatrix} I_{n'_B} & 0 \\ 0 & 0 \end{pmatrix}.$$

So the state $\frac{1}{2^{n_W/2}}\sum_{z\in\mathbb{F}_2^{n_W}}|A'z\rangle_{X,B}|z\rangle_W$ corresponds to the graph with many isolated edges and many isolated sites. Hence, it can be regarded as the state $|G'\rangle\otimes|+\rangle_{B'}\otimes|+\rangle_{W'}$.

Now, we have

$$\begin{aligned}
&\frac{1}{2^{n_W/2}}\sum_{z\in\mathbb{F}_2^{n_W}}|A'z\rangle_{X,B}|z\rangle_W\\
=&\frac{1}{2^{n_W/2}}\sum_{z\in\mathbb{F}_2^{n_W}}|C^{-1}ADz\rangle_{X,B}|z\rangle_W\\
=&\frac{1}{2^{n_W/2}}\sum_{z\in\mathbb{F}_2^{n_W}}|C^{-1}Az\rangle_{X,B}|D^{-1}z\rangle_W\\
=&U_{C^{-1},X,B}U_{D^{-1},Z,W}\frac{1}{2^{n_W/2}}\sum_{z\in\mathbb{F}_2^{n_W}}|Az\rangle_{X,B}|z\rangle_W\\
=&U_{C^{-1},X,B}U_{D^{-1},Z,W}|G\rangle\\
=&U_{C^T,Z,B}U_{D^T,X,W}|G\rangle\\
=&\frac{1}{2^{n_B/2}}\sum_{z\in\mathbb{F}_2^{n_B}}|z\rangle_B|A^Tz\rangle_{X,W}\\
=&\frac{1}{2^{n_B/2}}\sum_{z\in\mathbb{F}_2^{n_B}}|C^Tz\rangle_B|D^TA^Tz\rangle_{X,W}.
\end{aligned}$$

Hence, $|G\rangle$ can be converted to the state $|G'\rangle\otimes|+\rangle_{B'}\otimes|+\rangle_{W'}$ via the local unitary $U_{C^{-1},X,B}U_{D^{-1},Z,W}$. When we apply the Z measurement on W and the X measurement on B, the application of the unitary $U_{C^{-1},X,B}U_{D^{-1},Z,W}$ is equivalent with the application of the classical conversion $x\mapsto C^{-1}x$ and $z\mapsto D^{-1}z$. Similarly, when we apply the Z measurement on B and the X measurement on W, the application of the unitary $U_{C^{-1},X,B}U_{D^{-1},Z,W}$ is equivalent with the application of the classical conversion $x\mapsto D^Tx$ and $z\mapsto C^Tz$. Hence, applying these classical data conversions, we can treat the state $|G\rangle$ as the state $|G'\rangle\otimes|+\rangle_{B'}\otimes|+\rangle_{W'}$.

Appendix C: Concrete examples

Here, for a better understanding, we demonstrate the above results for few-qubit graph states.

1. Three-qubit graph state

Let us consider the case of the three-qubit graph state on $\bullet-\circ-\bullet$. We number the left black circle 1 and do the right black circle 2. Then, the matrix $A=\begin{pmatrix}1\\1\end{pmatrix}$. Then, $c_1=\begin{pmatrix}1\\1\end{pmatrix}$. Now, we have two choices for c_2, $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$. Then, we choose $c_2=\begin{pmatrix}1\\0\end{pmatrix}$, which implies that $C=\begin{pmatrix}1&1\\1&0\end{pmatrix}$ and $C^{-1}=\begin{pmatrix}0&1\\1&1\end{pmatrix}$. Also, we have $D=1$. Therefore, the required classical data conversions are given as follows. When we obtain X_1 and X_2 as the X measurement on B, and Z_1 the Z measurement on W, we need to use the data X_2, X_1+X_2, Z_1 instead of the original data. That is, we check whether the relation $X_2=Z_1$ holds. When we obtain Z_1 and Z_2 as the Z measurement on B, and X_1 the X measurement on W, we need to use the data Z_1+Z_2, Z_1, X_1 instead of the original data. That is, we check whether the relation $X_1=Z_1+Z_2$ holds.

2. Four-qubit graph state

Next, we consider the four-qubit graph state on the graph $\bullet-\circ-\bullet-\circ$. We number the left black circle 1 and do the right black circle 2. Similarly, we number the white circles. Then, the matrix $A=\begin{pmatrix}1&0\\1&1\end{pmatrix}$. Now, we choose $c_1=\begin{pmatrix}1\\1\end{pmatrix}$ and $c_2=\begin{pmatrix}0\\1\end{pmatrix}$, which implies that $C=A$ and $C^{-1}=\begin{pmatrix}1&0\\1&1\end{pmatrix}$. Also, we have $D=D^{-1}=I$. Therefore, the required classical data conversions are given as follows. When we obtain X_1 and X_2 as the X measurement on B, and Z_1 and Z_2 the Z measurement on W, we need to use the data X_1+X_2, X_2, Z_1, and Z_2 instead of the original data. That is, we check whether the relations $X_1+X_2=Z_1$ and $X_2=Z_2$ hold. When we obtain Z_1 and Z_2 as the Z measurement on B, and X_1 and X_2 the X measurement on W, we need to use the data Z_1, Z_1+Z_2, X_1, and X_2 instead of the original data. That is, we check whether the relations $X_1=Z_1$ and $X_2=Z_1+Z_2$ hold.

Appendix D: Analysis of the classical hypothesis testing problem

In this appendix, we show

Lemma 1 *When the distribution $\hat{P}$ satisfies*

$$\hat{P}(S_j=T_{k+j}=0 \text{ for } 1\le j\le k)\ge\ \alpha,$$

we have

$$\begin{aligned}
&\hat{P}(S_{2k+1}=T_{2k+1}=0|S_j=T_{k+j}=0 \text{ for } 1\le j\le k)\\
\ge\ &1-\frac{1}{\alpha(2k+1)}.
\end{aligned}$$

Here, $\hat{P}$ is a distribution on $2k+1$ trials, in which, each trial consists of two bits. Also, it is invariant for permutation of $2k+1$ trials.

Since Lemma 1 is the contraposition of Theorem 2 in the body, it is sufficient to show Lemma 1.

To address permutation-invariant distributions on $2k+1$ trials, we prepare the typical permutation-invariant distribution $\hat{P}_{a,b,c}$, in which, the possible numbers of events $(0,0)$, $(1,0)$, $(0,1)$, and $(1,1)$ are fixed to $2k+1-(a+b+c)$, a, b, and c, respectively. Hence, the real numbers a, b and c satisfy that $a,b,c \geq 0$ and $2k+1 \geq a+b+c$. Then, an arbitrary permutation-invariant distribution $\hat{P}$ is written as

$$\hat{P} = \sum_{a,b,c} Q(a,b,c) \hat{P}_{a,b,c}, \tag{D1}$$

where Q is a distribution on the set $\{(a,b,c)|a,b,c \geq 0, a+b+c \leq 2k+1\}$. In the following discussion, we consider the properties of typical permutation-invariant distributions $\hat{P}_{a,b,c}$ with the above condition for (a,b,c).

Consider the case when $c \geq 2$. Since we detect "1" at least once among $2k$ outcomes $S_1, \ldots, S_k, T_{k+1}, \ldots, T_{2k}$, we have

$$\hat{P}_{a,b,c}(S_j = T_{k+j} = 0 \text{ for } 1 \leq j \leq k) = 0.$$

Consider the case when $c = 1$. When $a \geq k+1$, we detect "1" at least once among k outcomes $T_{k+1}, \ldots, T_{2k}$ of X basis. Hence, we have

$$\hat{P}_{a,b,1}(S_j = T_{k+j} = 0 \text{ for } 1 \leq j \leq k) = 0. \tag{D2}$$

When $b \geq k+1$, we can show (D2) in the same way. Assume that $a, b \leq k$. To realize $S_j = T_{k+j} = 0$ for $1 \leq j \leq k$, the following conditions are required. a events $(1,0)$ occur from $k+1$-th trial to $2k$-th trial. b events $(0,1)$ occur from 1-th trial to k-th trial. One event $(1,1)$ occurs in $2k+1$-th trial. Hence, $k-a$ events $(0,0)$ occur from $k+1$-th trial to $2k$-th trial. $k-b$ events $(0,0)$ occur from 1st trial to k-th trial. In this case, the number of total cases is $\frac{(2k+1)!}{(2k-a-b)!a!b!}$. The number of cases satisfying the above conditions is $\frac{k!}{(k-a)!a!}\frac{k!}{(k-b)!b!}$. Hence, we have

$$\begin{aligned}
&\hat{P}_{a,b,1}(S_j = T_{k+j} = 0 \text{ for } 1 \leq j \leq k) \\
=&\frac{\frac{k!}{(k-a)!a!}\frac{k!}{(k-b)!b!}}{\frac{(2k+1)!}{(2k-a-b)!a!b!}} = \frac{k!k!(2k-a-b)!}{(2k+1)!(k-a)!(k-b)!} \\
=&\frac{1}{2k+1} \cdot \frac{k \cdots (k-a+1) \cdot k \cdots (k-b+1)}{(2k) \cdots (2k+1-a-b)} \\
\leq&\frac{1}{2k+1}.
\end{aligned} \tag{D3}$$

When $S_j = T_{k+j} = 0$ for $1 \leq j \leq k$, the event $(1,1)$ occurs in $2k+1$-th trial, i.e., $S_{2k+1} = T_{2k+1} = 1$. Thus,

$$\begin{aligned}
&\hat{P}_{a,b,1}(S_{2k+1} = T_{2k+1} = S_j = T_{k+j} = 0 \text{ for } 1 \leq j \leq k) \\
=&\hat{P}_{a,b,1}(S_{2k+1} = T_{2k+1} = 0 | S_j = T_{k+j} = 0 \text{ for } 1 \leq j \leq k) \\
=&0.
\end{aligned}$$

Consider the case when $c = 0$. When $a \geq k+2$ or $b \geq k+2$, similar to (D2), we can show that

$$\hat{P}_{a,b,0}(S_j = T_{k+j} = 0 \text{ for } 1 \leq j \leq k) = 0.$$

Assume that $a, b \leq k+1$. The condition $S_j = T_{k+j} = 0$ for $1 \leq j \leq k$ holds when one of the following three sets of conditions holds.

(1) $b-1$ events $(0,1)$ occur from 1st trial to k-th trial. a events $(1,0)$ occur from $k+1$-th trial to $2k$-th trial. The event $(0,1)$ occurs in $2k+1$-th trial.

(2) b events $(0,1)$ occur from 1st trial to k-th trial. $a-1$ events $(1,0)$ occur from $k+1$-th trial to $2k$-th trial. The event $(1,0)$ occurs in $2k+1$-th trial.

(3) b events $(0,1)$ occur from 1st trial to k-th trial. a events $(1,0)$ occur from $k+1$-th trial to $2k$-th trial. The event $(0,0)$ occurs in $2k+1$-th trial.

The numbers of cases of (1), (2), and (3) are $\binom{k}{(b-1)}\binom{k}{a}$, $\binom{k}{b}\binom{k}{(a-1)}$, and $\binom{k}{b}\binom{k}{a}$, respectively. Since the number of total cases is $\frac{(2k+1)!}{(2k+1-a-b)!a!b!}$. Hence, we have

$$\hat{P}_{a,b,0}(S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k) = \frac{\binom{k}{(b-1)}\binom{k}{a} + \binom{k}{b}\binom{k}{(a-1)} + \binom{k}{b}\binom{k}{a}}{\frac{(2k+1)!}{(2k+1-a-b)!a!b!}}$$
$$=\frac{(2k+1-a-b)!a!b!}{(2k+1)!}(k!)^2(\frac{1}{a!(b-1)!(k-a)!(k-b+1)!} + \frac{1}{(a-1)!b!(k-a+1)!(k-b)!} + \frac{1}{a!b!(k-a)!(k-b)!})$$
$$=\frac{(2k+1-a-b)!a!b!}{(2k+1)!}(k!)^2(\frac{b(k-a+1)}{a!b!(k-a+1)!(k-b+1)!} + \frac{a(k-b+1)}{a!b!(k-a+1)!(k-b+1)!} + \frac{(k-a+1)(k-b+1)}{a!b!(k-a+1)!(k-b+1)!})$$
$$=\frac{(2k+1-a-b)!a!b!}{(2k+1)!}(k!)^2\frac{b(k-a+1)+a(k-b+1)+(k-a+1)(k-b+1)}{a!b!(k-a+1)!(k-b+1)!}$$
$$=\frac{(2k+1-a-b)!a!b!}{(2k+1)!}(k!)^2\frac{(k+1)^2-ab}{a!b!(k-a+1)!(k-b+1)!}$$
$$=\frac{(2k+1-a-b)!a!b!}{(2k+1)!}\frac{((k+1)!)^2}{(k+1)^2}\frac{(k+1)^2-ab}{a!b!(k-a+1)!(k-b+1)!}$$
$$=\frac{(k+1)^2-ab}{(k+1)^2}\frac{(k+1)\cdots(k+2-a)\cdot(k+1)\cdots(k+2-b)}{(2k+1)\cdots(2k+2-a-b)}. \tag{D4}$$

Here, one might consider that $(k+1)^2$ can be canceled as a common factor. However, it is not true when a or b is zero. To keep the validity even in this case, we need to keep the term $(k+1)^2$ in the denominator.

Next, we proceed to $\hat{P}_{a,b,0}(S_{2k+1} = T_{2k+1} = 0, S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k)$. The conditions $S_1 = \ldots = S_k = T_{k+1} = \ldots = T_{2k} = 0$ holds when the conditions (3) holds. Hence, we have

$$\hat{P}_{a,b,0}(S_{2k+1} = T_{2k+1} = S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k)$$
$$=\frac{\binom{k}{b}\binom{k}{a}}{\frac{(2k+1)!}{(2k+1-a-b)!a!b!}}$$
$$=\frac{(2k+1-a-b)!a!b!}{(2k+1)!}\frac{(k!)^2}{a!b!(k-a)!(k-b)!}$$
$$=\frac{k!k!(2k+1-a-b)!}{(2k+1)!(k-a)!(k-b)!}$$
$$=\frac{k\cdots(k+1-a)\cdot k\cdots(k+1-b)}{(2k+1)\cdots(2k+2-a-b)}. \tag{D5}$$

Thus,

$$\hat{P}_{a,b,0}(S_{2k+1} = T_{2k+1} = 0 | S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k)$$
$$=\frac{(k+1-a)(k+1-b)}{(k+1)^2-ab}. \tag{D6}$$

In the following, we discuss the distribution Q instead of $\hat{P}$ because of (D1). Due to the above calculation, the event $S_j = T_{k+j} = 0$ for $1 \le j \le k$ occurs only when $c = 0, 1$. To evaluate the probability of this event, it is sufficient to consider the case of $c = 0, 1$. That is, we can restrict the support of the distribution Q to the case of $c = 0, 1$. Hence, using a parameter $\beta \in [0, 1]$ and a distribution Q_0 on the support $\{(a, b) | a + b \le 2k + 1, 0 \le a \le k + 1, 0 \le b \le k + 1\}$ and a distribution Q_1 on the support $\{(a, b) | 0 \le a \le k, 0 \le b \le k\}$, the distribution Q is written as

$$Q(a, b, c) = \begin{cases} \beta Q_0(a, b) & \text{if } c = 0 \\ (1-\beta)Q_1(a, b) & \text{if } c = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Define

$$T_1[Q_0] := \sum_{(a,b)} Q_0(a, b)\hat{P}_{a,b,0}(S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k)$$
$$T_2[Q_1] := \sum_{(a,b)} Q_1(a, b)\hat{P}_{a,b,1}(S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k),$$

and

$$T_3[Q_0]$$
$$:= \sum_{(a,b)} Q_0(a, b)\hat{P}_{a,b,0}\left(\begin{array}{l} S_{2k+1} = T_{2k+1} = S_j = T_{k+j} = 0 \\ \text{for } 1 \le j \le k \end{array} \right).$$

Then, we can show the following lemma.

Lemma 2 *Assume that*

$$\alpha > \frac{1}{2k+1}. \tag{D7}$$

When

$$\beta T_1[Q_0] + (1-\beta)T_2[Q_1] \ge \alpha. \tag{D8}$$

we have

$$\frac{\beta T_3[Q_0]}{\beta T_1[Q_0] + (1-\beta)T_2[Q_1]} \ge 1 - \frac{1}{\alpha(2k+1)}.$$

Since $\hat{P}(S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k) = \beta T_1[Q_0] + (1-\beta)T_2[Q_1]$ and $\hat{P}(S_{2k+1} = T_{2k+1} = 0 | S_j = T_{k+j} =$

0 for $1 \le j \le k) = \frac{\beta T_3[Q_0]}{\beta T_1[Q_0]+(1-\beta)T_2[Q_1]}$, Lemma 2 yields Lemma 1. Hence, it is sufficient to show Lemma 2.

The tightness of Lemma 2, i.e., that of Lemma 1, can be shown as follows. Assume that $\alpha < \frac{1}{2k+1}$, $\beta = 0$, and $Q_1(a,b) = \delta_{a,0}\delta_{b,0}$, which corresponds to the distribution $\hat{P}$ satisfying the following. The event $(1,1)$ occurs only in one event, and the remaining $2k$ events are $(0,0)$. Then, Eq. (D8) holds nevertheless $\frac{\beta T_3[Q_0]}{\beta T_1[Q_0]+(1-\beta)T_2[Q_1]} = 0$. That is, the distribution $\hat{P}$ breaks the condition $\hat{P}(S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k) \le \alpha$ nevertheless $\hat{P}(S_{2k+1} = T_{2k+1} = 0 | S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k) = 0$. Hence, the constraint $\alpha > \frac{1}{2k+1}$ is crucial. This situation corresponds to the following Bob's strategy. Bob generates $2k$ copies of the true state $|G\rangle$ and inserts only one bad state $\mathsf{W}_B^{x,z}|G\rangle$, where x, z are non-zero elements. Then, Bob can success the cheat with probability $\frac{1}{2k+1}$.

To show Lemma 2, we prepare the following lemma, which will be shown in the next section.

Lemma 3 *The relation*

$$\begin{aligned}&\frac{(k+1-a)(k+1-b)}{(k+1)^2-ab}\\ \ge& 1 - \frac{1}{2k+1}\frac{(k+1)^2}{(k+1)^2-ab}\\ &\times \frac{(2k+1)\cdots(2k+2-a-b)}{(k+1)\cdots(k+2-a)\cdot(k+1)\cdots(k+2-b)}\end{aligned} \tag{D9}$$

holds for $2k+1 \ge a+b$ *and* $k+1 \ge a, b \ge 0$.

Proof of Lemma 2: Due to (D3), we have

$$T_2[Q_1] \le \frac{1}{2k+1}. \tag{D10}$$

Hence, Condition (2) and (D7) imply that

$$\beta \ge \frac{\alpha - \frac{1}{2k+1}}{T_1[Q_0] - \frac{1}{2k+1}} \tag{D11}$$

and

$$T_1[Q_0] > \frac{1}{2k+1}. \tag{D12}$$

Due to the relations (D4) and (D6), Lemma 3 guarantees that

$$\begin{aligned}&\hat{P}_{a,b,0}(S_{2k+1} = T_{2k+1} = 0 | S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k)\\ \ge& 1 - \frac{1}{2k+1}\hat{P}_{a,b,0}(S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k)^{-1}\end{aligned}$$

when a and b satisfy the conditions $a+b \le 2k+1$, $0 \le a \le k+1$, and $0 \le b \le k+1$. Hence,

$$\begin{aligned}&\hat{P}_{a,b,0}(S_{2k+1} = T_{2k+1} = S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k)\\ \ge& \hat{P}_{a,b,0}(S_j = T_{k+j} = 0 \text{ for } 1 \le j \le k) - \frac{1}{2k+1}\end{aligned}$$

under the same condition. Taking the expectation for Q_0, we have

$$T_3[Q_0] \ge T_1[Q_0] - \frac{1}{2k+1}. \tag{D13}$$

Thus, we have

$$\begin{aligned}&\frac{\beta T_3[Q_0]}{\beta T_1[Q_0] + (1-\beta)T_2[Q_1]} \overset{(a)}{\ge} \frac{\beta T_3[Q_0]}{\beta T_1[Q_0] + \frac{(1-\beta)}{2k+1}}\\ \overset{(b)}{\ge}& \frac{T_3[Q_0]}{\alpha}\frac{\alpha - \frac{1}{2k+1}}{T_1[Q_0] - \frac{1}{2k+1}}\\ =& \frac{T_3[Q_0]}{T_1[Q_0] - \frac{1}{2k+1}}(1 - \frac{1}{\alpha(2k+1)}) \overset{(c)}{\ge} 1 - \frac{1}{\alpha(2k+1)}\end{aligned}$$

where (a) and (c) follow from (D10) and the combination of (D13) and (D12), respectively. The remaining part (b) follows from (D11) and the fact that $\frac{\beta T_1[Q_0]}{\beta T_1[Q_0]+\frac{(1-\beta)}{2k+1}} = \frac{T_1[Q_0]}{T_1[Q_0]+\frac{(\frac{1}{\beta}-1)}{2k+1}}$ is monotone increasing for β. ∎

Appendix E: Proof of Lemma 3

Define

$$\begin{aligned}&\xi(a,b,k)\\ :=&(k+1-a)(k+1-b) - (k+1)^2 + ab\\ &+ \frac{(k+1)^2\cdot(2k+1)\cdots(2k+2-a-b)}{(2k+1)\cdot(k+1)\cdots(k+2-a)\cdot(k+1)\cdots(k+2-b)}\\ =&\frac{(k+1)^2\cdot(2k)\cdots(2k+2-a-b)}{(k+1)\cdots(k+2-a)\cdot(k+1)\cdots(k+2-b)}\\ &-(a+b)k + 2ab - (a+b).\end{aligned}$$

Since (D9) is equivalent with $\xi(a,b,k) \ge 0$, we show the non-negativity of $\xi(a,b,k)$ in this section.

1. Organization

Before proceeding to the detailed analysis, we overview the organization of this section. We firstly show the non-negativity of $\xi(a,b,k)$ for the cases with $k = 1,2,3$ in Subsections E 2, E 3, and E 4. In the remaining subsection, we show it for the cases with $k \ge 4$. The detail organization can be summarized as follows. Without loss of generality, we can assume that $a \ge b$ due to the symmetry of $\xi(a,b,k)$. Remember that the relations $k+1 \ge a, b \ge 0$ and $2k+1 \ge a+b$ are also assumed.

a. *Cases:* $k = 1,2,3$

Combining discussions in Subsections E 2, E 3, and E 4, we can cover all of cases with $k = 1,2,3$ due to

the following reasons. The cases with $k = 1$ are composed of $(a, b) = (0, 0), (1, 0), (1, 1), (2, 0), (2, 1), (2, 2)$. The cases with $k = 2$ are composed of $(a, b) = (0, 0), (1, 0), (1, 1), (2, 0), (2, 1), (2, 2), (3, 0), (3, 1), (3, 2)$. These cases are covered in Subsection E 2.

The cases with $k = 3$ are composed of $(a, b) = (0, 0), (1, 0), (1, 1), (2, 0), (2, 1), (2, 2), (3, 0), (3, 1), (3, 2), (3, 3), (4, 0), (4, 1), (4, 2), (4, 3)$. In fact, the case with $(a, b, k) = (3, 3, 3)$ is covered in Subsection E 4, and the cases with $(a, b, k) = (4, 0, 3), (4, 1, 3), (4, 2, 3), (4, 3, 3)$ are covered in Subsection E 3. So, combining the cases discussed in Subsection E 2, we can show the cases with $k = 3$. So, we assume that $k \geq 4$ in the following discussion.

b. *Cases:* $a \leq 2$ *and* $k \geq 4$

The cases with $a \leq 2$ are covered in Subsection E 2.

c. *Cases:* $a + b \leq 5$ *and* $k \geq 4$

Many cases with $a + b \leq 5$ are covered in Subsection E 2. The remaining cases are $(a, b) = (4, 0), (4, 1), (5, 0)$. The cases $(a, b) = (4, 0), (5, 0)$ are covered in in Subsections E 5, and the case $(a, b) = (4, 1)$ is covered in in Subsections E 6.

d. *Cases:* $a + b \geq 6$, $a \geq 3$ *and* $k \geq 4$

The cases with $a+b \geq 6$, $a \geq 3$ and $k \geq 4$ are classified as Table I. Hence, all cases have been covered.

TABLE I: Cases with $a + b \geq 6$, $a \geq 3$ and $k \geq 4$

Subsection	Condition 1	Condition 2	Condition 3
E 7	$a = b$	$\frac{k+2}{2} \geq a$	-
E 8		$\frac{k+2}{2} < a$	-
E 9	$a \geq b + 1$	$\frac{k+2}{2} \geq b$	$b \geq 2$
E 5			$b = 0$
E 6			$b = 1$
E 10		$\frac{k+2}{2} < b$	-

2. Case: $(a, b) = (0, 0), (1, 0), (1, 1), (2, 0), (2, 1), (2, 2), (3, 0), (3, 1), (3, 2)$

Since the function $\xi(a, b, k)$ is symmetric for a and b, we consider only the case when $a \geq b$. For specific values (a, b), $\xi(a, b, k)$ can be calculated as follows.

$$\begin{aligned}
\xi(0, 0, k) &= \frac{(k+1)^2}{2k+1}, \\
\xi(1, 0, k) &= 0, \\
\xi(1, 1, k) &= 0, \\
\xi(2, 0, k) &= 0, \\
\xi(2, 1, k) &= k - 1, \\
\xi(2, 2, k) &= 4\frac{(k-1)^2}{k}, \\
\xi(3, 0, k) &= \frac{(k+1)^2}{k-1}, \\
\xi(3, 1, k) &= 4k - 2, \\
\xi(3, 2, k) &= \frac{11k^2 - 25k + 12}{k}.
\end{aligned}$$

The above values are non-negative when $k \geq a, b$.

3. Case: $a = k + 1$

$$\begin{aligned}
&\xi(k+1, b, k) \\
=&\frac{(2k)\cdots(k+1-b)}{k!(k\cdots(k+2-b))} - (k+1)^2 + b(k+1) \\
=&(k+1)(\frac{(2k)\cdots(k+1-b)}{k!((k+1)\cdots(k+2-b))} - (k+1-b)) \\
=&(k+1)(k+1-b)(\frac{(2k)\cdots(k+2-b)}{k!((k+1)\cdots(k+2-b))} - 1) \\
=&(k+1)(k+1-b)(\frac{(2k)\cdots(k+2)}{k!} - 1) \\
=&(k+1)(k+1-b)(\frac{(k+k)(k+k-1)\cdots(k+2)}{k(k-1)\cdot 2} - 1) \\
\geq&0.
\end{aligned}$$

4. Case: $(a, b) = (3, 3)$

$\xi(3, 3, k)$ can be calculated as follows.

$$\xi(3, 3, k) = \frac{2(k-2)}{k(k-1)}(13k^2 - 29k + 12). \quad \text{(E1)}$$

The case $(a, b) = (3, 3)$ is possible only when $k \geq 3$. It is positive in this case.

5. Case: $b = 0$ and $a \geq 2$

Since $\frac{2k\cdots(2k+2-a)}{k\cdots(k+2-a)} \geq 2^{a-1}$, we have

$$\begin{aligned}\xi(a,0,k) =& \frac{2k\cdots(2k+2-a)\cdot(k+1)}{k\cdots(k+2-a)} - a(k+1)\\ =&(k+1)(\frac{2k\cdots(2k+2-a)}{k\cdots(k+2-a)} - a)\\ \geq&(k+1)(2^{a-1}-a) \geq 0.\end{aligned}$$

6. Case: $b = 1$ and $a \geq 3$

Since the relations $\frac{(2k-2)\cdots(2k+1-a)}{(k-1)\cdots(k+2-a)} \geq 2^{a-2}$ and $\frac{2k-1}{k} \geq 1$ hold, we have

$$\begin{aligned}&\xi(a,1,k)\\ =&2k\frac{2k-1}{k}\frac{(2k-2)\cdots(2k+1-a)}{(k-1)\cdots(k+2-a)} - (a+1)k + a - 1\\ \geq&2^{a-1}k - (a+1)k + a - 1\\ =&(2^{a-1}-a-1)k + a - 1 \overset{(a)}{\geq} 0,\end{aligned}$$

where (a) follows from the inequality $a \geq 3$, respectively.

7. Case: $a = b$, $a \geq 3$, and $\frac{k+2}{2} \geq a$

We have

$$\begin{aligned}&\frac{(2k-1)(2k-2)\cdots(2k+5-2a)(2k+4-2a)}{((k-1)\cdots(k+2-a))^2}\\ \geq&2^{2(a-2)}.\end{aligned} \tag{E2}$$

Since $\frac{k+2}{2} \geq a$, we have

$$\frac{(2k+3-2a)}{k} \geq \frac{(2k+2-2a)}{k} \geq 1 \tag{E3}$$

Thus, the combination of (E2) and (E3) yields that

$$\begin{aligned}&\frac{2k\cdots(2k+2-2a)}{(k\cdots(k+2-a))^2}\\ =&2k\frac{(2k-1)(2k-2)\cdots(2k+5-2a)(2k+4-2a)}{((k-1)\cdots(k+2-a))^2}\\ &\times\frac{(2k+3-2a)(2k+2-2a)}{k^2}\\ \geq&2^{2(a-2)+1}k.\end{aligned} \tag{E4}$$

Therefore,

$$\begin{aligned}\xi(a,a,k) =& \frac{2k\cdots(2k+2-2a)}{(k\cdots(k+2-a))^2} - 2ak + 2(a^2-a)\\ \overset{(a)}{\geq}&2^{2(a-2)+1}k - 2ak + 2(a^2-a)\\ =&(2^{2(a-2)+1}-2a)k + 2(a^2-a) \overset{(b)}{\geq} 0,\end{aligned}$$

where (a) and (b) follow from (E4) and the inequality $a \geq 3$, respectively.

8. Case: $a = b$, $k \geq a > \frac{k+2}{2}$, and $k \geq 4$

Firstly, we show

$$\begin{aligned}&\frac{(2k-1)(2k-2)\cdots k}{(k(k-1)\cdots(\lfloor\frac{k}{2}\rfloor+1))\cdot(k(k-1)\cdots(\lceil\frac{k}{2}\rceil+1))}\\ \geq&2^{k-2}.\end{aligned} \tag{E5}$$

When k is an even number $2s$,

$$\begin{aligned}&\frac{(2k-1)(2k-2)\cdots k}{(k(k-1)\cdots(\lfloor\frac{k}{2}\rfloor+1))\cdot(k(k-1)\cdots(\lceil\frac{k}{2}\rceil+1))}\\ =&\frac{(4s-1)(4s-2)\cdots(2s)}{((s2)(2s-1)\cdots(s+1))^2}\\ =&\frac{(4s-1)(4s-3)\cdots(2s+1)}{(2s)(2s-1)\cdots(s+1)}\frac{(4s-2)(4s-4)\cdots(2s)}{(2s)(2s-1)\cdots(s+1)}\\ \geq&\frac{(4s-1)(4s-3)\cdots(2s+3)}{(2s-1)(2s-2)\cdots(s+1)}\frac{(4s-2)(4s-4)\cdots(2s+2)}{(2s-1)(2s-2)\cdots(s+1)}\\ \geq&2^{s-1}\cdot 2^{s-1} = 2^{2s-2} = 2^{k-2}.\end{aligned}$$

When k is an odd number $2s+1$,

$$\begin{aligned}&\frac{(2k-1)(2k-2)\cdots k}{(k(k-1)\cdots(\lfloor\frac{k}{2}\rfloor+1))\cdot(k(k-1)\cdots(\lceil\frac{k}{2}\rceil+1))}\\ =&\frac{(4s+1)(4s)\cdots(2s+1)}{(((2s+1)(2s)\cdots(s+1)\cdot(2s+1)(2s)\cdots(s+2)))}\\ =&\frac{(4s+1)(4s-1)\cdots(2s+1)}{(2s+1)(2s)\cdots(s+1)}\frac{(4s)(4s-2)\cdots(2s+2)}{(2s+1)(2s)\cdots(s+2))}\\ \geq&\frac{(4s+1)(4s-1)\cdots(2s+3)}{(2s)(2s-1)\cdots(s+1)}\frac{(4s)(4s-2)\cdots(2s+4)}{(2s)(2s-1)\cdots(s+2))}\\ \geq&2^s\cdot 2^{s-1} = 2^{2s-1} = 2^{k-2}.\end{aligned}$$

Hence, we obtain (E5).

Considering the even and odd cases in the same way, we can show that

$$\frac{(k-1)\cdots(2k+2-2a)}{(\lfloor\frac{k}{2}\rfloor\cdots(k+2-a))\cdot(\lceil\frac{k}{2}\rceil\cdots(k+2-a))} \geq 1. \tag{E6}$$

The condition $k \geq a > \frac{k+2}{2}$ implies that $a \geq \lceil\frac{k}{2}\rceil + 1$. Hence, we have

$$\lfloor\frac{k}{2}\rfloor + 1 \geq k + 2 - a. \tag{E7}$$

Combining (E5), (E6), and (E7), we have

$$\begin{aligned}&\frac{2k\cdots(2k+2-2a)}{(k\cdots(k+2-a))^2}\\ =&2k\frac{(2k-1)(2k-2)\cdots(k+2)(k+1)k}{(k(k-1)\cdots(\lfloor\frac{k}{2}\rfloor+1))\cdot(k(k-1)\cdots(\lceil\frac{k}{2}\rceil+1))}\\ &\times\frac{(k-1)\cdots(2k+2-2a)}{(\lfloor\frac{k}{2}\rfloor\cdots(k+2-a))\cdot(\lceil\frac{k}{2}\rceil\cdots(k+2-a))}\\ \geq&2k\frac{(2k-1)(2k-2)\cdots(k+2)(k+1)k}{(k(k-1)\cdots(\lfloor\frac{k}{2}\rfloor+1))\cdot(k(k-1)\cdots(\lceil\frac{k}{2}\rceil+1))}\\ \geq&2k2^{k-2}.\end{aligned} \tag{E8}$$

Thus,

$$\begin{aligned}\xi(a,a,k) &= \frac{2k\cdots(2k+2-2a)}{(k\cdots(k+2-a))^2} - 2ak + 2(a^2-a)\\ &\overset{(a)}{\geq} 2k2^{k-2} - 2ak + 2(a^2-a) = 2(2^{k-2}-a)k + 2(a^2-a)\\ &\overset{(b)}{\geq} 2(2^{k-2}-k)k + 2(a^2-a) \overset{(c)}{\geq} 0,\end{aligned}$$

where (a), (b), and (c) follow from (E8), the inequality $k \geq a$, and the inequality $k \geq 4$, respectively.

9. Case: $\frac{k+1}{2} \geq b \geq 2$ and $a \geq b+1$ and $a+b \geq 6$

Since the above cases cover all of cases with $a+b \leq 5$, we can assume that $a+b \geq 6$ in the following discussion as well as $k \geq 4$, $b \geq 2$. Since $b \geq 2$ and $a \geq b+1$, we have the following calculation.

$$\begin{aligned}&2k\frac{(2k-1)(2k-3)\cdots(2k+3-2b)}{k(k-1)\cdots(k+2-b)}\frac{(2k-2)(2k-4)\cdots(2k+2-2b)}{k(k-1)\cdots(k+2-b)}\frac{(2k+1-2b)(2k-2b)\cdots(2k+2-a-b)}{(k+1-b)(k-b)\cdots(k+2-a)}\\ =&2k\frac{(2k-1)(2k-3)\cdots(2k+5-2b)}{(k-1)(k-2)\cdots(k+2-b)}\frac{(2k+3-2b)}{k}\frac{(2k-2)(2k-4)\cdots(2k+4-2b)}{(k-1)(k-2)\cdots(k+2-b)}\\ &\times\frac{(2k+2-2b)}{k}\frac{(2k+1-2b)}{(k+1-b)}\frac{(2k-2b)\cdots(2k+2-a-b)}{(k-b)\cdots(k+2-a)}\\ =&2k\frac{(2k-1)(2k-3)\cdots(2k+5-2b)}{(k-1)(k-2)\cdots(k+2-b)}\frac{(2k-2)(2k-4)\cdots(2k+4-2b)}{(k-1)(k-2)\cdots(k+2-b)}\frac{(2k+2-2b)}{k}\\ &\times\frac{(2k-2b)\cdots(2k+2-a-b)}{(k-b)\cdots(k+2-a)}\frac{(2k+3-2b)}{k}\frac{(2k+1-2b)}{(k+1-b)}\\ =&2k\frac{(2k-1)(2k-3)\cdots(2k+5-2b)}{(k-1)(k-2)\cdots(k+2-b)}\frac{(2k-2)(2k-4)\cdots(2k+4-2b)}{(k-1)(k-2)\cdots(k+2-b)}\frac{(2k+2-2b)}{k}\\ &\times\frac{(2k-2b)\cdots(2k+2-a-b)}{(k-b)\cdots(k+2-a)}\frac{(2k+1-2b)}{k}\frac{(2k+3-2b)}{(k+1-b)}\\ \overset{(a)}{\geq}&2k\cdot 2^{b-2}\cdot 2^{b-2}\cdot 2^{(a-b-1)}\cdot 2 = 2^{a+b-3}k,\end{aligned} \tag{E9}$$

where (a) follows the following relations. We have $\frac{(2k-1)(2k-3)\cdots(2k+5-2b)}{(k-1)(k-2)\cdots(k+2-b)} \geq 2^{b-2}$, $\frac{(2k-2)(2k-4)\cdots(2k+4-2b)}{(k-1)(k-2)\cdots(k+2-b)} = 2^{b-2}$, $\frac{(2k+2-2b)}{k} \geq 1$, $\frac{(2k+1-2b)}{k} \geq 1$, and $\frac{(2k+3-2b)}{(k+1-b)} \geq 2$. Also, the assumption guarantees the relation $a \geq 2$, which implies that $\frac{(2k-2b)\cdots(2k+2-a-b)}{(k-b)\cdots(k+2-a)} \geq 2^{(a-b-1)}$.

Hence,

$$\begin{aligned}\xi(a,b,k) =& \frac{2k\cdots(2k+2-a-b)}{(k\cdots(k+2-a))\cdot(k\cdots(k+2-b))}\\ &-(a+b)k + (2ab-a-b)\\ =&\frac{2k\cdots(2k+2-a-b)}{(k\cdots(k+2-a))\cdot(k\cdots(k+2-b))}\\ &-(a+b)k + (2ab-a-b)\\ \overset{(b)}{\geq}&(2^{a+b-3}-(a+b))k + (2ab-a-b) \overset{(c)}{\geq} 0.\end{aligned}$$

where (b) and (c) follow from (E9) and the inequality $a+b \geq 6$, respectively.

10. Case: $b > \frac{k+1}{2}$, $k \geq a \geq b+1$, and $k \geq 4$

The condition $b > \frac{k}{2}+1$ implies $b \geq k+1-\lfloor\frac{k}{2}\rfloor$. Hence, we have $\lfloor\frac{k}{2}\rfloor + 1 \geq (k+2-b)$. Thus, we have

$$\begin{aligned}&\frac{(2k-1)(2k-3)\cdots(2k+3-2b)}{k(k-1)\cdots(k+2-b)}\\ \geq&\frac{(2k-1)(2k-3)\cdots(2\lfloor\frac{k}{2}\rfloor+1)}{k(k-1)\cdots(\lfloor\frac{k}{2}\rfloor+1)}\\ =&\frac{(2k-1)(2k-3)\cdots(2\lfloor\frac{k}{2}\rfloor+2)}{(k-1)(k-2)\cdots(\lfloor\frac{k}{2}\rfloor+1)}\frac{(2\lfloor\frac{k}{2}\rfloor+1)}{k} \geq 2^{k-\lfloor\frac{k}{2}\rfloor-1}.\end{aligned}$$

Since $b \geq k+1-\lceil\frac{k}{2}\rceil$ implies $(\lceil\frac{k}{2}\rceil+1) \geq (k+2-b)$, we have

$$\begin{aligned}&\frac{(2k-2)(2k-4)\cdots(2k+2-2b)}{k(k-1)\cdots(k+2-b)}\\ \geq&\frac{(2k-2)(2k-4)\cdots(2\lceil\frac{k}{2}\rceil)}{k(k-1)\cdots(\lceil\frac{k}{2}\rceil+1)}\\ =&\frac{(2k-2)(2k-4)\cdots(2\lceil\frac{k}{2}\rceil+2)}{(k-1)(k-2)\cdots(\lceil\frac{k}{2}\rceil+1)}\frac{(2\lceil\frac{k}{2}\rceil)}{k} \geq 2^{k-\lceil\frac{k}{2}\rceil-1}.\end{aligned}$$

Hence,

$$\begin{aligned}
&\frac{2k\cdots(2k+2-a-b)}{(k\cdots(k+2-a))\cdot(k\cdots(k+2-b))}\\
=&2k\frac{(2k-1)(2k-3)\cdots(2k+3-2b)}{k(k-1)\cdots(k+2-b)}\\
&\times\frac{(2k-2)(2k-4)\cdots(2k+2-2b)}{k(k-1)\cdots(k+2-b)}\\
&\times\frac{(2k+1-2b)(2k-2b)\cdots(2k+2-a-b)}{(k+1-b)(k-b)\cdots(k+2-a)}\\
\geq&2k\frac{(2k-1)(2k-3)\cdots(2k+3-2b)}{k(k-1)\cdots(k+2-b)}\\
&\times\frac{(2k-2)(2k-4)\cdots(2k+2-2b)}{k(k-1)\cdots(k+2-b)}\\
\geq&2k\cdot 2^{k-\lfloor\frac{k}{2}\rfloor-1}\cdot 2^{k-\lceil\frac{k}{2}\rceil-1}\\
=&2^{2k-\lfloor\frac{k}{2}\rfloor-\lceil\frac{k}{2}\rceil-1}k=2^{k-1}k. \qquad \text{(E10)}
\end{aligned}$$

Thus, we have

$$\begin{aligned}
&\xi(a,b,k)\\
=&\frac{2k\cdots(2k+2-a-b)}{(k\cdots(k+2-a))\cdot(k\cdots(k+2-b))}\\
&-(a+b)k+(2ab-a-b)\\
\overset{(a)}{\geq}&2^{k-1}k-(a+b)k+(2ab-a-b)\\
=&(2^{k-1}-(a+b))k+(2ab-a-b)\\
\overset{(b)}{\geq}&(2^{k-1}-2k+1)k+(2ab-a-b)\overset{(c)}{\geq}0,
\end{aligned}$$

where (a), (b), and (c) follow from (E10), the inequality $a+b\leq 2k-1$, and the inequality $k\geq 4$, respectively.

[1] R. Raussendorf and H. J. Briegel, A one-way quantum computer. Phys. Rev. Lett. **86**, 5188 (2001).

[2] A. Broadbent, J. F. Fitzsimons, and E. Kashefi, Universal blind quantum computation. Proc. of the 50th Annual IEEE Sympo. on Found. of Comput. Sci. 517 (2009).

[3] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Demonstration of blind quantum computing. Science **335**, 303 (2012).

[4] Of course, there are some unavoidable leakages, such as the upper bound of the Alice's computing size, etc.

[5] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, Composable security of delegated quantum computation. Adv. in Crypt. ASIACRYPT 2014, Lecture Notes in Comput. Sci. **8874**, 406 (2014).

[6] T. Morimae and K. Fujii, Blind quantum computation for Alice who does only measurements. Phys. Rev. A **87**, 050301(R) (2013).

[7] V. Dunjko, E. Kashefi, and A. Leverrier, Blind quantum computing with weak coherent pulses. Phys. Rev. Lett. **108**, 200502 (2012).

[8] M. Hajdusek, C. A. Perez-Delgado, and J. F. Fitzsimons, Device-independent verifiable blind quantum computation. arXiv:1502.02563

[9] A. Gheorghiu, E. Kashefi, and P. Wallden, Robustness and device independence of verifiable blind quantum computing. arXiv:1502.02571

[10] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind computation. arXiv:1203.5217.

[11] T. Morimae, Verification for measurement-only blind quantum computing. Phys. Rev. A **89**, 060302(R) (2014).

[12] T. Morimae, V. Dunjko, and E. Kashefi, Ground state blind quantum computation on AKLT state. Quant. Inf. Comput. **15**, 0200 (2015).

[13] T. Morimae and K. Fujii, Blind topological measurement-based quantum computation. Nat. Comm. **3**, 1036 (2012).

[14] T. Morimae, Continuous-variable blind quantum computation. Phys. Rev. Lett. **109**, 230502 (2012).

[15] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Efficient universal blind computation. Phys. Rev. Lett. **111**, 230501 (2013).

[16] A. Mantri, C. Pérez-Delgado, and J. F. Fitzsimons, Optimal blind quantum computation. Phys. Rev. Lett. **111**, 230502 (2013).

[17] Q. Li, W. H. Chan, C. Wu, and Z. Wen, Triple-server blind quantum computation using entanglement swapping. Phys. Rev. A **89**, 040302(R) (2014).

[18] T. Sueki, T. Koshiba, and T. Morimae, Ancilla-driven universal blind quantum computation. Phys. Rev. A **87**, 060301(R) (2013).

[19] T. Morimae and K. Fujii, Secure entanglement distillation for double-server blind quantum computation. Phys. Rev. Lett. **111**, 020502 (2013).

[20] C. A. Perez-Delgado and J. F. Fitzsimons, Overcoming efficiency constraints on blind quantum computation. arXiv:1411.4777

[21] R. Raussendorf, J. Harrington, and K. Goyal, Topological fault-tolerance in cluster state quantum computation. New. J. Phys. **9**, 199 (2007).

[22] D. Gross and J. Eisert, Novel schemes for measurement-based quantum computation. Phys. Rev. Lett. **98**, 220503 (2007).

[23] G. K. Brennen and A. Miyake, Measurement-based quantum computer in the gapped ground state of a two-body Hamiltonian. Phys. Rev. Lett. **101**, 010502 (2008).

[24] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems. Nature. **496**, 456 (2013).

[25] M. McKague, Interactive proofs for BQP via self-tested graph states. arXiv:1309.5675

[26] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Experimental verification of quantum computation. Nature Phys. **9**, 727 (2013).

[27] To our knowledge, the first paper that uses the direct verification of the graph state in the client-server context is Ref. [25].

[28] E. L. Lehmann and J. P. Romano, *Testing Statistical Hy-*

potheses. Springer Texts in Statistics, Springer (2008).
[29] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction. Phys. Rev. A, **54**, 3824 (1996).
[30] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier, Self-testing of quantum circuits. Automata, Languages and Programming, Lecture Notes in Comput. Sci. **4051**, 72 (2006).
[31] W. van Dam, F. Magniez, M. Mosca, and M. Santha, Self-testing of universal and fault-tolerant sets of quantum gates. Proc. of the 32nd Ann. ACM Symp. on Theor. of Comput. (STOC2000), 688 (2000).
[32] M. Hayashi, S. Ishizaka, A. Kawachi, G. Kimura, and T. Ogawa, *Introduction to Quantum Information Science*, Graduate Texts in Physics, Springer (2014).
[33] M. Hayashi, K. Matsumoto, and Y. Tsuda, A study of LOCC-detection of a maximally entangled state using hypothesis testing, J. Phys. A: Math. Gen. **39**, 14427-14446 (2006).
[34] M. Hayashi, Group theoretical study of LOCC-detection of maximally entangled state using hypothesis testing, New J. Phys. **11**, 043028 (2009).
[35] M. Owari and M. Hayashi, Two-way classical communication remarkably improves local distinguishability, New J. Phys. **10**, 013006 (2008).
[36] M. Owari, and M. Hayashi, Asymptotic local hypothesis testing between a pure bipartite state and the completely mixed state, Phys. Rev. A **90**, 032327 (2014).
[37] M. Owari, and M. Hayashi, Local hypothesis testing between a pure bipartite state and the white noise state, IEEE Transactions on Information Theory **61**(12), pp.6995-7011 (2015).
[38] M. Hayashi, and M. Owari, Tight asymptotic bounds on local hypothesis testing between a pure bipartite state and the white noise state, IEEE International Symposium on Information Theory (ISIT2015), Hong Kong, June 14 - June 19, 2015. pp. 691-695 (2015).
[39] E. Alba, G. Toth, J. J. Garcia-Ripoll, Phys. Rev. A **82**, 062321 (2010).
[40] J. Joo, E. Alba, J. J. Garcia-Ripoll, T. P. Spiller, Phys. Rev. A **88**, 012328 (2013).
[41] A. Gheorghiu, E. Kashefi, and P. Wallden, Robustness and device independence of verifiable blind quantum computing. arXiv:1502.02571
[42] M. Hajdusek, C. A. Perez-Delgado, and J. F. Fitzsimons, Device-independent verifiable blind quantum computation. arXiv:1502.02563