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
(Received 4 June 2015; published 25 November 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 get 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 the stabilizers of some copies.

DOI: 10.1103/PhysRevLett.115.220502 PACS numbers: 03.67.Ac, 03.67.Dd

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 *et al.* [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 the 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 state generation, single-qubit measurement [6] or coherent state 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 measurement 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 of her messages to Bob whatever they do on their systems. Quantum physics respects the no-signaling principle.

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

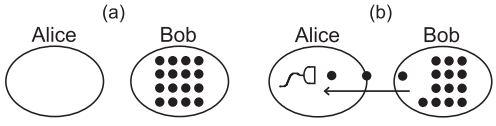

FIG. 1. The measurement-only blind quantum computing. (a) Bob generates a resource state. (b) Bob sends Alice each qubit of the resource state one by one. Alice adaptively measures each qubit.

pursuing the completely classical client is an important direction, in particular, for the goal of constructing an interactive proof of Bounded Quantum Polytime, where the assumption of noncommunicating multiprovers is natural, in this Letter we restrict ourselves to the single-server setup assuming some minimum quantum technologies for the client, since in the context of blind quantum computing, assuming 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 us to derive a more practical bound suitable for experiments. The 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 state generation, 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 Letter, 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 $k = \mathrm{poly}(n)$. The graph state $|G\rangle$ is defined by $|G\rangle \equiv (\bigotimes_{e\in E} \mathrm{CZ}_e)|+\rangle^{\otimes n}$, where $|+\rangle \equiv 1/\sqrt{2}(|0\rangle + |1\rangle)$, E is the set of edges of G, and CZ_e is the CONTROLLED-Z gate $\mathrm{CZ} \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$ 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 $j = 1, 2, \ldots, n$, 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 [28,29], 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 Letter (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 the first section of the Supplemental Material [30].

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 [Figs. 2(a) and 2(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.

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

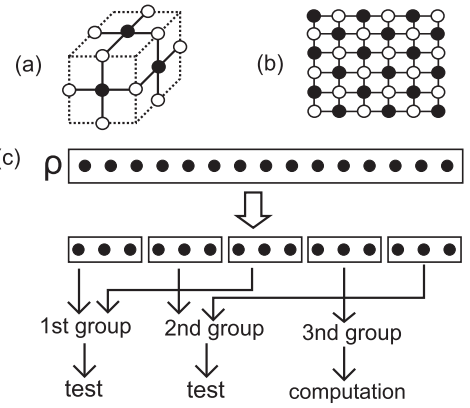

FIG. 2. (a) The RHG lattice. (b) An example of bipartite graphs: the two-dimensional square lattice. Black and white colors indicate the bipartitions B and W, respectively. (c) An example for $n = 3$, $k = 2$. Two blocks go to the first group, and the other two blocks go to the second group. The left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

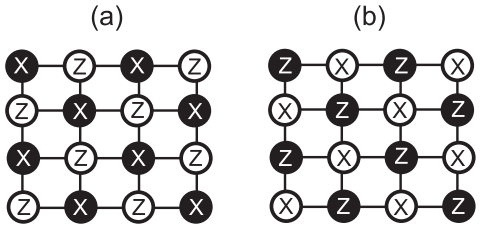

FIG. 3. An example for the two-dimensional square lattice. The measurement pattern for the first group (a) and the second group (b).

outcome in the X basis that violates the stabilizer relations is obtained, Alice rejects.

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 $\alpha > [1/(2k+1)]$. If the test is passed, with significance level α, we can guarantee that the resultant state σ of the third group satisfies

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

[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 Eq. (1) [39].] The proof of the theorem is given below and in the Supplemental Material [30]. From the theorem and the relation between the fidelity and trace norm [40][(6.106)], we can conclude the verifiability: if Alice passes the test, she can guarantee

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

for any POVM C with the significance level α. If we take $\alpha = [1/(\sqrt{2k+1})]$, for example, the left-hand side of the above inequality is $[1/(2k+1)^{1/4}] \to 0$ if $k \to \infty$, and, therefore, the verifiability is satisfied. Note that the lower bound, $\alpha > [1/(2k+1)]$, 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 $1/(2k+1)$, which corresponds to $\alpha = [1/(2k+1)]$.

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 [41]. (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 $\mathcal{K}_W$ have 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 measurement based on Alice's original bases, Alice can realize the measurement based on above modified bases. The detail of this discussion is given in Sec. II of the Supplemental Material [30].

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

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

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

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

Thus, the discrete-twirled state

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

satisfies $\mathrm{Tr}(\bar{\rho}|G'\rangle\langle G'|^{\otimes 2k+1}) = \mathrm{Tr}(\rho|G'\rangle\langle G'|^{\otimes 2k+1})$ [41]. Also, we have

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

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 $(\mathsf{W}_B^{\mathbf{x},\mathbf{z}} \otimes \mathsf{W}_W^{-\mathbf{z},-\mathbf{x}})\bar{\rho}(\mathsf{W}_B^{\mathbf{x},\mathbf{z}} \otimes \mathsf{W}_W^{-\mathbf{z},-\mathbf{x}})^\dagger = \bar{\rho}$ and ρ is permutation invariant, the state $\bar{\rho}$ is written with a permutation-invariant distribution P on $\mathbb{F}_2^{2n'_B(2k+1)}$ as [41]

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

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 notation 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 ith measurement outcome of the X basis of the B system coincides with the prediction by the ith measurement outcome of the Z basis of the 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 the X basis of the W system coincides with the prediction by the $k+i$th measurement outcome of the Z basis of the B system. So, to show Theorem 1, it is enough to show the following theorem.

Theorem 2: Assume that $\alpha > [1/(2k+1)]$. When the distribution $\hat{P}$ satisfies

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

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 the Supplemental Material [30].

M. H. is partially supported by the JSPS Grant-in-Aid for Scientific Research (A) Grant No. 23246071 and the National Institute of Information and Communication Technology, 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. T. M. is supported by the JSPS Grant-in-Aid for Young Scientists (B) Grant No. 26730003 and the MEXT JSPS Grant-in-Aid for Scientific Research on Innovative Areas Grant No. 15H00850.

[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, in *Proceedings of the 50th Annual IEEE Symposium on Foundation of Computer Science*, 2009, p. 517.
[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 Alice's computing size, etc.
[5] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, Composable security of delegated quantum computation, Lect. Notes 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, New J. Phys. **17**, 083040 (2015).
[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, Quantum Inf. Comput. **15**, 0200 (2015).
[13] T. Morimae and K. Fujii, Blind topological measurement-based quantum computation, Nat. Commun. **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, Phys. Rev. Lett. **114**, 220502 (2015).
[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 (London) **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, Nat. 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] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier, Self-testing of quantum circuits, Lect. Notes Comput. Sci. **4051**, 72 (2006).
[29] W. van Dam, F. Magniez, M. Mosca, and M. Santha, Self-testing of universal and fault-tolerant sets of quantum gates, in *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC2000)*, 2000, p. 688.
[30] See the Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.115.220502, which includes Refs. [31–38], for details of proofs.
[31] M. Hayashi, K. Matsumoto, and Y. Tsuda, A study of LOCC-detection of a maximally entangled state using hypothesis testing, J. Phys. A **39**, 14427 (2006).
[32] M. Hayashi, Group theoretical study of LOCC-detection of maximally entangled state using hypothesis testing, New J. Phys. **11**, 043028 (2009).
[33] M. Owari and M. Hayashi, Two-way classical communication remarkably improves local distinguishability, New J. Phys. **10**, 013006 (2008).
[34] 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).
[35] M. Owari and M. Hayashi, Local hypothesis testing between a pure bipartite state and the white noise state, arXiv:1006.2744.
[36] M. Hayashi and M. Owari, Tight asymptotic bounds on local hypothesis testing between a pure bipartite state and the white noise state, in *Proceedings of the IEEE International Symposium on Information Theory (ISIT2015)*, Hong Kong, 2015, pp. 691–695.
[37] E. Alba, G. Toth, andJ. J. Garcia-Ripoll, Mapping the spatial distribution of entanglement in optical lattices, Phys. Rev. A **82**, 062321 (2010).
[38] J. Joo, E. Alba, J. J. Garcia-Ripoll, and T. P. Spiller, Generating and verifying graph states for fault-tolerant topological measurement-based quantum computing in two-dimensional optical lattices, Phys. Rev. A **88**, 012328 (2013).
[39] E. L. Lehmann and J. P. Romano, *Testing Statistical Hypotheses,* Springer Texts in Statistics (Springer, New York, 2008).
[40] M. Hayashi, S. Ishizaka, A. Kawachi, G. Kimura, and T. Ogawa, *Introduction to Quantum Information Science*, Graduate Texts in Physics (Springer, New York, 2014).
[41] 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).