PHYSICAL REVIEW A **89**, 060302(R) (2014)

Verification for measurement-only blind quantum computing

Tomoyuki Morimae
ASRLD Unit, Gunma University, 1-5-1 Tenjin-cho, Kiryu-shi, Gunma 376-0052, Japan
and Department of Physics, Imperial College London, London SW7 2AZ, United Kingdom
(Received 23 October 2013; revised manuscript received 30 May 2014; published 17 June 2014)

Blind quantum computing is a new secure quantum computing protocol where a client who does not have any sophisticated quantum technology can delegate her quantum computing to a server without leaking any privacy. It is known that a client who has only a measurement device can perform blind quantum computing [T. Morimae and K. Fujii, Phys. Rev. A **87**, 050301(R) (2013)]. It has been an open problem whether the protocol can enjoy the verification, i.e., the ability of the client to check the correctness of the computing. In this paper, we propose a protocol of verification for the measurement-only blind quantum computing.

DOI: 10.1103/PhysRevA.89.060302 PACS number(s): 03.67.Dd

I. INTRODUCTION

Blind quantum computing [1–10] is a secure delegated quantum computing, where a client (Alice), who does not have enough quantum technology, delegates her quantum computing to a server (Bob), who has a fully fledged quantum computer, without leaking any information about her computation to Bob. A blind quantum computing protocol for almost classical Alice was first proposed by Broadbent, Fitzsimons, and Kashefi [1] by using the measurement-based model due to Raussendorf and Briegel [11]. In their protocol, Alice only needs a device which emits randomly rotated single-qubit states. Later it was shown that weak coherent pulses, instead of single-photon states, are sufficient for blind quantum computation [5]. Recently, it was shown that blind quantum computing can be verifiable [2,9,10]. Here, verifiable means that Alice can test Bob's computation [2,9,10]. The verifiability is an important requirement, since Alice cannot recalculate the result of the delegated computation by herself to check the correctness (remember that she does not have any quantum computer), and therefore if there is no verification method, she might be palmed off with a wrong result by a fishy company who tries to sell a fake quantum computer [9,10]. The verifiable blind protocol was experimentally demonstrated with a photonic qubit system [9,10].

Recently, another type of blind quantum computing protocol was proposed in Ref. [3]. In this protocol, Alice needs only a device that can measure quantum states. One advantage of this protocol is that the security is device independent [12–16], and is based on the no-signaling principle [17], which is more fundamental than quantum physics. However, it has been an open problem whether the protocol can enjoy verification.

In this paper, we propose a verification protocol for the measurement-only blind quantum computing. We will propose two protocols. Interestingly, our protocols are based on the combination of two different concepts from different fields: the no-signaling principle [17] from the foundation of physics and the topological quantum error correcting code [18–20] from a practical application in quantum information. The no-signaling principle means that a shared quantum (or more general) state cannot be used to transmit information. It is one of the most central principles in physics, and known to be more fundamental than quantum physics (i.e., there is a theory which is more nonlocal than quantum physics but does not violate the no-signaling principle [17]). The topological quantum error correcting code is a specific type of the quantum error correcting code which cleverly uses the topological order of exotic quantum symmetry-breaking systems to globally encode logical states.

II. TOPOLOGICAL MEASUREMENT-BASED QUANTUM COMPUTATION

The Raussendorf-Harrington-Goyal state $|\mathrm{RHG}\rangle$ is the three-dimensional graph state with the elementary cell given in Fig. 1(a). Defects in the graph state are created by Z measurements on $|\mathrm{RHG}\rangle$ as usual in the cluster measurement-based model. Topological braidings of defect tubes can implement some Clifford gates [18–20]. Non-Clifford gates, that are necessary for the universal quantum computation, are implemented by the magic state preparation and distillation [21]. A string of Z operators acting on the resource state, which has at least one open edge, is considered as an error, and its edge(s) is detected by syndrome measurements of cubicles of X operators [Fig. 1(b)]. A string of Z operators on the resource states, which connects or surrounds defects [Fig. 1(c)], is not detected, and can be a logical error. Local adaptive measurements can implement quantum computation as well as syndrome error detection.

III. FIRST PROTOCOL

Let us explain our first protocol. The basic idea of our protocol is illustrated in Fig. 2: Bob prepares the resource state, and Alice performs measurements.

More precisely, our protocol runs as follows (Fig. 3). First, Bob prepares a universal resource state, and sends each qubit of it to Alice one by one [Fig. 3(a)]. Alice measures each qubit until she remotely creates the N-qubit state, $\sigma_q|\Psi_P\rangle$, in Bob's laboratory [Fig. 3(b)], where $\sigma_q \equiv \bigotimes_{j=1}^{N} X_j^{x_j} Z_j^{z_j}$ with $q \equiv (x_1,\ldots,x_N,z_1,\ldots,z_N) \in \{0,1\}^{2N}$ is the by-product of the measurement-based quantum computation [11], and X_j and Z_j are Pauli operators acting on jth qubit. The state $|\Psi_P\rangle \equiv P(|R\rangle \otimes |+\rangle^{\otimes N/3} \otimes |0\rangle^{\otimes N/3})$ is the N-qubit state, where $|R\rangle$ is an $N/3$-qubit universal resource state of the measurement-based quantum computation encoded with a quantum error-correcting code of the code distance d. (The size

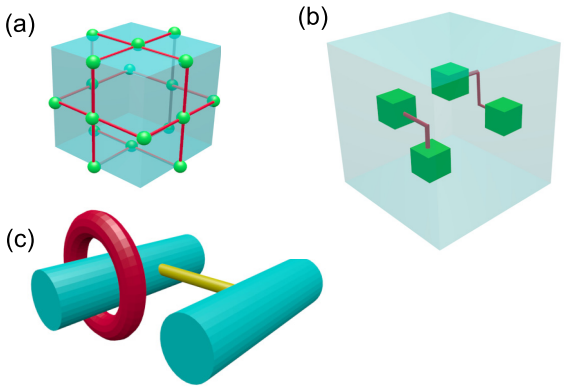

FIG. 1. (Color online) Topological measurement-based quantum computation. (a) The elementary cell of the Raussendorf-Harrington-Goyal state. Green balls are qubits, and red bonds are controlled-Z gates. (b) The error detection. Red strings are errors. Green boxes are syndrome operators. (c) Undetected errors or logical operations. Blue tubes are defects. Red and yellow strings are strings of operators, which surround or connect defects, respectively.

of $|R\rangle$ and the number of traps are optimal, since if there are too many traps, the efficiency of the computation becomes small, whereas if there are too few traps, the probability of detecting malicious Bob becomes small.) For example, $|R\rangle$ can be the $N/3$-qubit Raussendorf-Harrington-Goyal state [18,19] with sufficiently many magic states being already distilled. (The Raussendorf-Harrington-Goyal state is the resource state of the topological measurement-based quantum computing [18,19]. Instead of the RHG state, any other quantum error-correcting code can be utilized. Therefore, we can also assume that $|R\rangle$ is a normal resource state of the measurement-based quantum computation encoded with a quantum error-correcting code.) We define $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and P is an N-qubit permutation, which keeps the order of qubits in $|R\rangle$. This permutation is randomly chosen by Alice and kept secret to Bob.

Throughout this paper, we assume that there is no communication channel from Alice to Bob. Then, due to the no-signaling principle, Bob cannot learn anything about P [3]. If Bob can learn something about P, Alice can transmit some message to Bob by encoding her message into P, which contradicts the no-signaling principle.

Bob sends each qubit of $\sigma_q|\Psi_P\rangle$ to Alice one by one, and Alice does the measurement-based quantum computation on $\sigma_q|\Psi_P\rangle$ with correcting σ_q [Fig. 3(c)]. This means that before

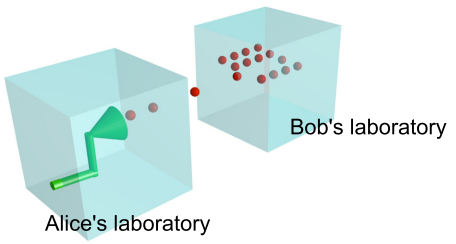

FIG. 2. (Color online) Our setup. Bob first prepares a resource state. Bob next sends each particle to Alice one by one. Alice measures each particle according to her algorithm.

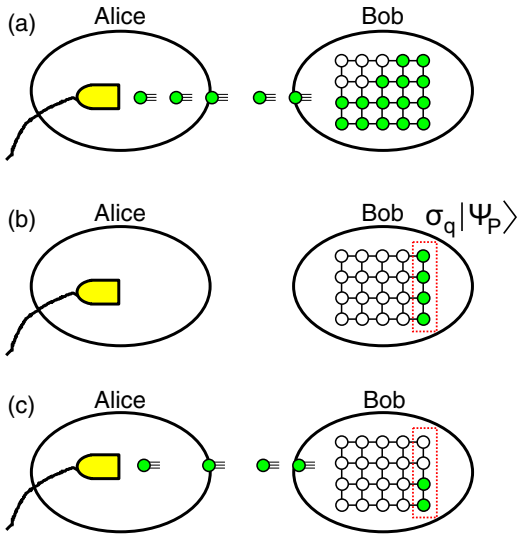

FIG. 3. (Color online) Our protocol. Here, $|\Psi_P\rangle \equiv P(|R\rangle \otimes |+\rangle^{\otimes N/3} \otimes |0\rangle^{\otimes N/3})$, P is a N-qubit permutation, and $|R\rangle$ is a universal resource state.

measuring jth qubit of $\sigma_q|\Psi_P\rangle$ she applies $\sigma_q^\dagger|_j$ on jth qubit, where $\sigma_q^\dagger|_j$ is the restriction of $\sigma_q^\dagger$ on jth qubit. For example, $(I \otimes XZ \otimes Z)|_2 = XZ$. Qubits belonging to $|R\rangle$ are used to implement Alice's desired quantum computation. States $|0\rangle$ and $|+\rangle$ are used as "traps" [2]. In other words, she measures Z on $|0\rangle$ and X on $|+\rangle$, and if she obtains the minus result (i.e., $|1\rangle$ or $|-\rangle$ state), she aborts the protocol. If results are plus for all traps, she accepts the result of the measurement-based quantum computation on $|R\rangle$.

IV. VERIFIABILITY

Now we show that if all measurements on traps show the correct results, the probability that a logical state of Alice's computation is changed is exponentially small. In other words, the probability that Alice is fooled by Bob is exponentially small. Hence our protocol is verifiable.

Since Bob might be dishonest, he might deviate from the above procedure. His general attack is a creation of a different state ρ instead of $\sigma_q|\Psi_P\rangle$. If he is honest, $\rho = \sigma_q|\Psi_P\rangle\langle\Psi_P|\sigma_q^\dagger$. If he is not honest, ρ can be any state. However, for any N-qubit state ρ, there exists a completely positive-trace-preserving (CPTP) map which satisfies $\rho = \sum_j E_j\sigma_q|\Psi_P\rangle\langle\Psi_P|\sigma_q^\dagger E_j^\dagger$, where $E_j \equiv \sum_\alpha C_j^\alpha \sigma_\alpha$, is a Kraus operator of the CPTP map, and C_j^α is a complex number (see Appendix A). Since $E_j^\dagger E_j$ is a POVM, $I = \sum_j E_j^\dagger E_j = \sum_j \sum_{\alpha,\beta} C_j^{\alpha *} C_j^\beta \sigma_\alpha^\dagger \sigma_\beta$, we obtain $\sum_j \sum_\alpha |C_j^\alpha|^2 = 1$.

Bob does not know q. Therefore, from Bob's viewpoint, the state is averaged over all q:

$$\frac{1}{4^N}\sum_q \sum_j \sigma_q^\dagger E_j \sigma_q |\Psi_P\rangle\langle\Psi_P|\sigma_q^\dagger E_j^\dagger \sigma_q$$

$$= \frac{1}{4^N}\sum_q \sum_{j,\alpha,\beta} C_j^\alpha C_j^{\beta *} \sigma_q^\dagger \sigma_\alpha \sigma_q |\Psi_P\rangle\langle\Psi_P|\sigma_q^\dagger \sigma_\beta^\dagger \sigma_q$$

$$= \frac{1}{4^N}\sum_q\sum_{j,\alpha}\left|C_j^\alpha\right|^2\sigma_q^\dagger\sigma_\alpha\sigma_q|\Psi_P\rangle\langle\Psi_P|\sigma_q^\dagger\sigma_\alpha^\dagger\sigma_q$$
$$= \sum_{j,\alpha}\left|C_j^\alpha\right|^2\sigma_\alpha|\Psi_P\rangle\langle\Psi_P|\sigma_\alpha^\dagger$$
$$= \sum_\alpha \tilde{C}_\alpha\sigma_\alpha|\Psi_P\rangle\langle\Psi_P|\sigma_\alpha^\dagger, \quad (1)$$

where $\tilde{C}_\alpha \equiv \sum_j |C_j^\alpha|^2$ and $\sum_\alpha \tilde{C}_\alpha = \sum_\alpha\sum_j |C_j^\alpha|^2 = 1$. Here, we have used the following equations [22]:

$$\sum_q \sigma_q^\dagger\sigma_\alpha\sigma_q\rho\sigma_q^\dagger\sigma_\beta^\dagger\sigma_q = 0,$$
$$\frac{1}{4^N}\sum_q \sigma_q^\dagger\sigma_\alpha\sigma_q\rho\sigma_q^\dagger\sigma_\alpha^\dagger\sigma_q = \sigma_\alpha\rho\sigma_\alpha^\dagger, \quad (2)$$

for any ρ and $\alpha \neq \beta$. The second equation is easy to show. For a proof of Eq. (2), see Appendix B. Equation (1) shows that we can assume that Bob's attack is the "random Pauli" attack, i.e., Bob randomly applies Pauli operators on each qubit.

Bob's attacks after creating ρ can also be included in the preparation of ρ. This is understood as follows. Let us assume that, after creating ρ, Bob sends a subsystem S_1 of ρ to Alice, and then Alice measures all particles of S_1. After Alice's measurement, Bob might apply an operation on another subsystem S_2 of ρ which has not been sent to Alice. However, Bob cannot know Alice's measurement angles and results on S_1 due to the no-signaling principle, and therefore Bob's operation on S_2 is independent of Alice's measurements on S_1. Furthermore, Bob's operation on S_2 commutes with Alice's measurements on S_1. Hence we can consider as if Bob applied such an operation on S_2 immediately after he preparing ρ.

In short, we can assume that Bob's attack is a random Pauli attack on the correct state $|\Psi_P\rangle$ as is shown in Eq. (1). Hence let us focus on $\sigma_\alpha|\Psi_P\rangle$. For many quantum error-correcting codes (such as the topological one [18,19]), if the weight $|\alpha|$ of σ_α is less than a certain integer d (the code distance), then such an error is detected or does not change logical states [2,18–20]. For example, in the topological code, d is determined by the defect thickness and distance between defects [18,19]. Here, the weight $|\alpha|$ of σ_α means the number of nontrivial operators in σ_α. (For example, the weight of $I\otimes XZ\otimes Z\otimes I\otimes X$ is 3.) Therefore, in order for σ_α to change a logical state of the computation, $|\alpha|$ must be larger than d. (To understand it, let us consider a simple example. If we encode the logical 0 as $|0_L\rangle \equiv |000\rangle$ and the logical 1 as $|1_L\rangle \equiv |111\rangle$, we must flip more than two qubits to change the logical state. A single bit flip is detected and corrected when the majority vote is done.)

Alice randomly chooses a permutation P. In this case, the probability of $P^\dagger\sigma_\alpha P$ not changing any trap is at most $(\frac{2}{3})^{|\alpha|/3}$. (For a calculation, see Appendix C.) Therefore, the probability that the logical state is changed and no trap is flipped is at most $\sum_{|\alpha|\geqslant d}\tilde{C}_\alpha(\frac{2}{3})^{|\alpha|/3} \leqslant (\frac{2}{3})^{d/3}\sum_{|\alpha|\geqslant d}\tilde{C}_\alpha \leqslant (\frac{2}{3})^{d/3}$, where we have used the fact $\tilde{C}_\alpha \geqslant 0$ and $\sum_{|\alpha|\geqslant d}\tilde{C}_\alpha \leqslant \sum_\alpha \tilde{C}_\alpha = 1$. Here, we have said "at most," since the above sum includes the contribution from σ_α which has a weight larger than d but does not contain any logical error. In this way, we have shown that the probability that Alice is fooled by Bob is exponentially small (d can be sufficiently large by concatenating the code). As we have seen, no communication from Alice to Bob is required for the verification. Therefore, whatever Alice's measurement device does, Bob cannot learn Alice's computational information because of the no-signaling principle. In other words, the security of the protocol is device independent.

V. SECOND PROTOCOL

Let us explain our second protocol, which uses the property of the topological code, and does not use any trap. Alice randomly chooses $k \equiv (h_1,\ldots,h_N,t_1,\ldots,t_N) \in \{0,1\}^{2N}$, and defines the N-qubit operator $K_k \equiv \bigotimes_{j=1}^N T_j^{t_j}H_j^{h_j}$, where $T \equiv |0\rangle\langle 0| + i|1\rangle\langle 1|$ and H is the Hadamard operator. Note that $T^\dagger XT = -iXZ, T^\dagger ZT = Z$, and $T^\dagger XZT = -iX$. Next, Alice defines the N-qubit state $|\Psi_k\rangle \equiv K_k|\mathrm{RHG}'\rangle$, where $|\mathrm{RHG}'\rangle$ is the N-qubit Raussendorf-Harrington-Goyal state [18,19] with a sufficient number of magic states being already distilled [18,19].

Bob prepares a universal resource state, and sends each qubit of it to Alice one by one. Alice does measurements and creates $\sigma_q|\Psi_k\rangle$ in Bob's laboratory, where σ_q is the by-product of the measurement-based quantum computation. Due to the no-signaling principle, Bob cannot learn k. Bob sends each qubit of $\sigma_q|\Psi_k\rangle$ to Alice one by one, and Alice does her topological measurement-based quantum computation with correcting $\sigma_q K_k$. If Alice detects any error, she aborts the protocol.

Again, because of Eq. (1), we can assume that Bob's attack is a random Pauli attack. Therefore, let us focus on $\sigma_\alpha|\Psi_k\rangle$. In order for σ_α to change a logical state without being detected by syndrome measurements, σ_α must contain at least one string s_α of operators which connects or surrounds defects [Fig. 1(c)] [18–20]. Since Alice randomly chooses k, the probability that all operators in $K_k^\dagger s_\alpha K_k$ become Z or XZ operators is at most $(\frac{3}{4})^{|s_\alpha|}$, where $|s_\alpha|$ is the weight of s_α. Note that $|s_\alpha| \geqslant d$ because it connects or surrounds defects.

Hence the probability that the logical state is changed and Alice does not detect any error is at most $\sum_{|\alpha|\geqslant d}\tilde{C}_\alpha(\frac{3}{4})^{|s_\alpha|} \leqslant (\frac{3}{4})^d\sum_{|\alpha|\geqslant d}\tilde{C}_\alpha \leqslant (\frac{3}{4})^d$. In short, our second protocol is also verifiable. Again, the device-independent security is guaranteed by the no-signaling principle.

ACKNOWLEDGMENTS

The author acknowledges support by JSPS and Tenure Track System by MEXT Japan.

APPENDIX A: EXISTENCE OF A CPTP MAP

Let $\{|\phi_k\rangle\}_{k=1}^{2^N}$ be any orthonormal basis of the N-qubit Hilbert space, $\langle\phi_k|\phi_j\rangle = \delta_{k,j}$. We diagonalize the N-qubit state ρ as $\rho = \sum_{j=1}^{2^N}\lambda_j|\lambda_j\rangle\langle\lambda_j|$. Let us take $E_{jk} \equiv \sqrt{\lambda_j}|\lambda_j\rangle\langle\phi_k|$. Then for any N-qubit state $\eta = \sum_{\alpha,\beta}\eta_{\alpha\beta}|\phi_\alpha\rangle\langle\phi_\beta|$, $\sum_{j,k}E_{jk}\eta E_{jk}^\dagger = \sum_{j,k,\alpha,\beta}\sqrt{\lambda_j}\sqrt{\lambda_j}\eta_{\alpha\beta}|\lambda_j\rangle\langle\phi_k|\phi_\alpha\rangle\langle\phi_\beta|\phi_k\rangle$

$\langle\lambda_j| = \sum_{j,k} \lambda_j \eta_{kk} |\lambda_j\rangle\langle\lambda_j| = \rho$. Furthermore, $\sum_{j,k} E_{jk}^\dagger E_{jk} = \sum_{j,k} \sqrt{\lambda_j}\sqrt{\lambda_j}|\phi_k\rangle\langle\lambda_j|\lambda_j\rangle\langle\phi_k| = \sum_{j,k} \lambda_j |\phi_k\rangle\langle\phi_k| = I$.

APPENDIX B: PROOF OF EQ. (2)

For the convenience of readers, we here give the proof [22] of Eq. (2). Since $\alpha \neq \beta$, there exists an index j such that $\sigma_\alpha|_j \neq \sigma_\beta|_j$. For any such $\sigma_\alpha|_j$ and $\sigma_\beta|_j$, we can always take $S \in \{X, Z\}$ such that S anticommutes only one of $\sigma_\alpha|_j$ and $\sigma_\beta^\dagger|_j$. Let us define $Q \equiv I^{\otimes j-1} \otimes S \otimes I^{\otimes N-j}$. Then, $\sum_q \sigma_q^\dagger \sigma_\alpha \sigma_q \rho \sigma_q^\dagger \sigma_\beta^\dagger \sigma_q = \sum_q (Q\sigma_q)^\dagger \sigma_\alpha (Q\sigma_q) \rho (Q\sigma_q)^\dagger \sigma_\beta^\dagger (Q\sigma_q) = \sum_q (\sigma_q^\dagger Q^\dagger) \sigma_\alpha (Q\sigma_q) \rho (\sigma_q^\dagger Q^\dagger) \sigma_\beta^\dagger (Q\sigma_q) = -\sum_q \sigma_q^\dagger \sigma_\alpha \sigma_q \rho \sigma_q^\dagger \sigma_\beta^\dagger \sigma_q$.

APPENDIX C: PROBABILITY OF AVOIDING TRAPS

Let $\sigma_\alpha|_j$ be the restriction of σ_α for jth qubit. [For example, $(X \otimes I \otimes XZ)|_3$ is XZ.] Let a, b, c be the number of j such that $\sigma_\alpha|_j = X$, Z, XZ, respectively. (In other words, a is the number of X operators in σ_α, b is the number of Z operators in σ_α, and c is the number of XZ operators in σ_α.) We define $|\alpha|$ as the weight of σ_α, namely, the number of non-I operators. Since $|\alpha| = a + b + c \leqslant 3\max(a,b,c)$, we obtain $\max(a,b,c) \geqslant \frac{|\alpha|}{3}$.

Let us assume $\max(a,b,c) = a$. Then, the probability that all X operators of σ_α do not change any trap is $\frac{(N-a)!\prod_{k=0}^{a-1}(\frac{2N}{3}-k)}{N!} = (\frac{2}{3})^a \frac{\prod_{k=0}^{a-1}(N-\frac{3}{2}k)}{\prod_{k=0}^{a-1}(N-k)} \leqslant (\frac{2}{3})^a \leqslant (\frac{2}{3})^{|\alpha|/3}$. This is larger than the probability that σ_α does not change any trap.

We can obtain the same result for $\max(a,b,c) = b$. For $\max(a,b,c) = c$, we have only to replace $\frac{2}{3}$ with $\frac{1}{3}$.

[1] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 2009), pp. 517–526.
[2] J. F. Fitzsimons and E. Kashefi, arXiv:1203.5217.
[3] T. Morimae and K. Fujii, Phys. Rev. A **87**, 050301(R) (2013).
[4] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
[5] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).
[6] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, arXiv:1301.3662.
[7] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Phys. Rev. Lett. **111**, 230501 (2013).
[8] A. Mantri, C. A. Pérez-Delgado, and J. F. Fitzsimons, Phys. Rev. Lett. **111**, 230502 (2013).
[9] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Nat. Phys. **9**, 727 (2013).
[10] T. Morimae, Nat. Phys. **9**, 693 (2013).
[11] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[12] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[13] V. Scarani, Acta Phys. Slov. **62**, 347 (2012).
[14] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. Lett. **110**, 010503 (2013).
[15] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. A **86**, 062326 (2012).
[16] M. McKague and L. Sheridan, arXiv:1209.4696.
[17] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[18] R. Raussendorf, J. Harrington, and K. Goyal, New. J. Phys. **9**, 199 (2007).
[19] R. Raussendorf, J. Harrington, and K. Goyal, Ann. Phys. (NY) **321**, 2242 (2006).
[20] A. Kitaev, Ann. Phys. (NY) **303**, 2 (2003).
[21] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[22] D. Aharonov, M. Ben-Or, and E. Eban, *Proceedings of Innovations in Computer Science* (Tsinghua University Press, Beijing, 2010), p. 453.