PHYSICAL REVIEW A **89**, 040302(R) (2014)

Triple-server blind quantum computation using entanglement swapping

Qin Li,[1] Wai Hong Chan,[2] Chunhui Wu,[3] and Zhonghua Wen[1]
[1]*College of Information Engineering, Xiangtan University, Xiangtan 411105, China*
[2]*Department of Mathematics and Information Technology, The Hong Kong Institute of Education, Hong Kong*
[3]*Department of Computer Science, Guangdong University of Finance, Guangzhou 510521, China*
(Received 28 January 2014; published 18 April 2014)

Blind quantum computation allows a client who does not have enough quantum resources or technologies to achieve quantum computation on a remote quantum server such that the client's input, output, and algorithm remain unknown to the server. Up to now, single- and double-server blind quantum computation have been considered. In this work, we propose a triple-server blind computation protocol where the client can delegate quantum computation to three quantum servers by the use of entanglement swapping. Furthermore, the three quantum servers can communicate with each other and the client is almost classical since one does not require any quantum computational power, quantum memory, and the ability to prepare any quantum states and only needs to be capable of getting access to quantum channels.

DOI: 10.1103/PhysRevA.89.040302 PACS number(s): 03.67.Ac, 03.67.Dd, 03.67.Lx, 03.65.Ud

Quantum computation, which is based on the principles of quantum mechanics to implement computation, provides a considerable speed advantage over its classical counterparts [1]. For instance, quantum computers can efficiently simulate quantum mechanical systems that are too difficult to simulate on classical computers [2]; in particular, Shor's algorithms for factorizing big integers and solving discrete logarithm problems are exponentially faster than their best-known classical algorithms [3] and Grover's algorithm for searching offers a quadratic speedup over its best-known classical counterparts [4]. However, the experimental realization of quantum computation is extremely challenging. Although various physical systems such as optical photons, cavity quantum electrodynamics devices, ion traps, nuclear spins, and superconducting equipments are considered to build quantum computers, all of them just allow for several operations on a few qubits at present. It is still a long way to build large-scale quantum computers. Thus, in the future the use of the first-generation quantum computers will be likely to adopt the "cloud" style [5]; that is, a small number of costly quantum servers only available in academia, corporations, and governments will be accessed by a great number of clients who have limited computational resources or power. These clients (Alices) would like to delegate their computational problems that have no efficient solutions on classical computers to quantum servers (Bobs), but also want to keep their inputs, outputs, and algorithms private. Blind quantum computation (BQC) can help them achieve the two goals at the same time.

The first BQC protocol was proposed by Childs using the quantum circuit model [6]. However, in this protocol, Alice is required to own quantum memory and be able to implement the SWAP gate. Then Arrighi and Salvail devised a BQC protocol where Alice just needs to prepare and measure entangles states [7]. However, the protocol is not a universal one since it only allows for calculating the classical functions that admit an efficient procedure to produce random input-output pairs. Broadbent, Fitzsimons, and Kashefi presented the first universal BQC protocol, as well as the first protocol in which Alice does not require any quantum computation power and memory and only requires preparing single-qubit states [8]. Furthermore, the protocol has already been experimentally demonstrated by performing a series of blind computations on four-qubit blind cluster states [9]. Thereafter, various BQC protocols have been devised to be as practical as possible [10–17], such as making Alice as classical as possible or tolerating more faults. The composable security of these protocols also has been studied [18,19].

All of the above-mentioned BQC protocols are single-server protocols and need the client to meet some least-possible quantum requirements, such as the ability to produce single-qubit states or make measurements. Actually, in Ref. [8], Broadbent, Fitzsimons, and Kashefi pointed out that their single-server BQC protocol can be modified to be a double-server BQC protocol. In such a double-server protocol, Alice can be completely classical if the two delegated quantum servers (Bob1 and Bob2) who share Bell states are assumed to be noncommunicating. Moreover, Morimae and Fujii ingeniously achieved entanglement distillation even if the two entangled servers are not allowed to communicate with each other and modified the double-server protocol in Ref. [8] to adapt to the case after entanglement distillation [20]. However, it is unrealistic to prevent two powerful quantum servers from communicating and it had been an open problem whether such a demanding requirement can be removed. In this work, we solve the problem and show that the client Alice can delegate her quantum computation to quantum servers who can communicate mutually while keeping her data secret. The cost is that three quantum servers need to be used and Alice needs to have quantum channels between her and the three servers.

Before giving our triple-server BQC protocol, we review the single-server BQC protocol in Ref. [8] and the modified double-sever BQC protocol in Ref. [20] separately. Suppose that the client Alice has in mind the quantum computation on the m-qubit graph state corresponding to the graph G. The specific operation she intends to carry out is to measure the ith qubit in the basis $\{|\pm\phi_i\rangle = |0\rangle \pm e^{i\phi_i}|1\rangle\}$, where $\phi_i \in S \equiv \{k\pi/4|k = 0,1,\ldots,7\}$. Then the single-server BQC protocol can be briefly described as follows. (S1) Alice prepares m qubits and sends them to the server Bob. The state of each qubit

is $|\theta_i\rangle = |0\rangle + e^{i\theta_i}|1\rangle (i = 1,2,\ldots,m)$, where θ_i is uniformly chosen from the set S. (S2) Alice asks Bob to generate a brickwork state according to the graph G specified by her. (S3) Bob produces the brickwork state $|G(\theta)\rangle$ by applying controlled-Z gates on the received qubits based on the graph G. (S4) For $i = 1,2,\ldots,m$, Alice randomly chooses r_i and computes $\delta_i = (\theta_i + \phi_i' + r_i\pi) \mod 2\pi$, where ϕ_i' is obtained according to the previous measurements and ϕ_i, and then δ_i is sent to Bob if Alice needs Bob to measure the ith qubit of $|G(\theta)\rangle$. (S5) Bob performs a measurement on the ith ($i = 1,2,\ldots,m$) qubit in the basis $\{|\pm\delta_i\rangle\}$ and informs Alice about the measurement result.

This single-sever BQC protocol can be modified to be a BQC protocol with authentication where a cheating server can be found with great probability and to be a double-server BQC protocol in which Alice can be totally classical. More details can be found in Ref. [8].

In the double-server BQC protocol in Ref. [8] and the modified version in Ref. [20], completely classical Alice, who only has to own a classical computer and two classical channels, can delegate her quantum computation to two quantum servers (Bob1 and Bob2) while keeping her data private. We briefly review the modified double-server BQC protocol in Ref. [20] without entanglement distillation as follows. (D1) A trusted center distributes m Bell states $\bigotimes_{i=0}^{m}|\psi_{z_i,x_i}\rangle$ to Bob1 and Bob2, where $|\psi_{z_i,x_i}\rangle = (I\otimes X^{x_i}Z^{z_i})(|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}$, $(z_i,x_i)\in\{0,1\}^2$, $X = |0\rangle\langle 1| + |1\rangle\langle 0|$, and $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. (D2) Alice randomly chooses m classical messages $\{\tilde{\theta}_i = (-1)^{x_i}\theta_i + z_i\pi\}_{i=1}^{m}$ from the set S^m and sends them to Bob1. (D3) Bob1 measures his part of the ith ($i = 1,2,\ldots,m$) Bell state in the basis $|\pm\tilde{\theta}_i\rangle$ and records the measurement result as $b_i\in\{0,1\}$. Note that after the measurement, the state of the corresponding part held by Bob2 is changed as $|\theta_i + b_i\pi\rangle$. (D4) When Bob1 finishes all the measurements, he sends Alice the measurement results $\{b_i\}_{i=1}^{m}$. (D5) Alice starts the reviewed single-server BQC protocol with Bob2 from step S2, replacing θ_i with $\theta_i + b_i\pi$ ($i = 1,2,\ldots,m$). Note that it is essential to require the two quantum servers Bob1 and Bob2 to be noncommunicating in the above double-server BQC protocol; otherwise the security of Alice's private data cannot be guaranteed [8,20].

In order to construct the triple-server BQC protocol, we will employ the technique of entanglement swapping [21–25], which is very useful in various quantum information applications such as quantum teleportation [26,27], quantum repeaters [28,29], and quantum cryptography [30,31]. This technique can let two unrelated particles be entangled. We first give a brief introduction of entanglement swapping and then present the triple-server BQC protocol and analyze its security.

The four Bell states are chosen as entanglement resources. Let the state of a pair of particles (a, b) be denoted by $|\psi_{z,x}(a,b)\rangle = (I\otimes X^xZ^z)(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b)/\sqrt{2}$, where $(z,x)\in\{0,1\}^2$, $X = |0\rangle_b\langle 1| + |1\rangle_b\langle 0|$, and $Z = |0\rangle_b\langle 0| - |1\rangle_b\langle 1|$. Considering two pairs of particles (a, b) and (a', b'), they are in the Bell states $|\psi_{z,x}(a,b)\rangle$ and $|\psi_{z',x'}(a',b')\rangle$, respectively. Now we perform a joint measurement on particles b and b' in the Bell basis [32] and then the combined state of particles a and a' is projected onto one of the four Bell states depending on the result of the Bell state measurement on particles b and b'. A pictorial description of the above process of entanglement swapping is shown in Fig. 1.

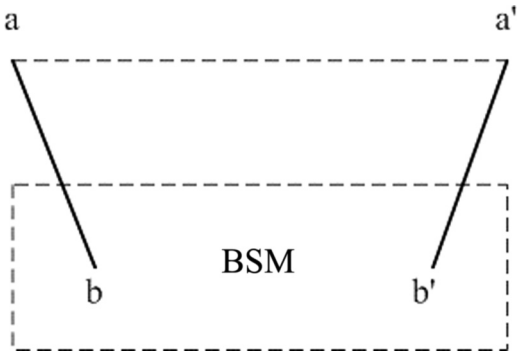

FIG. 1. Process of entanglement swapping. The solid lines connect particles in Bell states, the dashed rectangle denotes the Bell state measurement (BSM) on the two particles, and the dashed line connects the other two particles in a different Bell state after the Bell state measurement is made.

Without loss of generality, we will let the state of particles a and b be $|\psi_{0,0}(a,b)\rangle$ and the state of particles a' and b' be $|\psi_{0,0}(a',b')\rangle$. So the combined state of the four particles is $|\psi(a,b,a',b')\rangle = |\psi_{0,0}(a,b)\rangle\otimes|\psi_{0,0}(a',b')\rangle$, which can be rewritten in the following form:

$$\begin{aligned}|\psi(a,b,a',b')\rangle &= \tfrac{1}{2}[|\psi_{0,0}(a,a')\rangle|\psi_{0,0}(b,b')\rangle + |\psi_{0,1}(a,a')\rangle|\psi_{0,1}(b,b')\rangle \\ &\quad + |\psi_{1,0}(a,a')\rangle|\psi_{1,0}(b,b')\rangle + |\psi_{1,1}(a,a')\rangle|\psi_{1,1}(b,b')\rangle].\end{aligned} \tag{1}$$

When particles b and b' are measured in the Bell basis, i.e., projected onto one of the four Bell states, particles a and a' will collapse to the corresponding Bell state. For instance, if the measurement result is $|\psi_{0,0}(b,b')\rangle$, the state of particles a and a' is $|\psi_{0,0}(a,a')$. Note that we will label each measurement result as two classical bits, i.e., $|\psi_{0,0}(b,b')\rangle$ as (0,0), $|\psi_{0,1}(b,b')\rangle$ as (0,1), $|\psi_{1,0}(b,b')\rangle$ as (1,0), and $|\psi_{1,1}(b,b')\rangle$ as (1,1). This is because classical information is easy to transmit and store.

Now we begin to present the triple-server BQC protocol where the almost classical Alice wants to delegate her quantum computation to three quantum servers, Bob1, Bob2, and Bob3, and still keep her input, output, and procedure hidden from the servers. The almost classical Alice means that she does not need any quantum computational power, quantum memory, and the ability to prepare any quantum states and she only has to own quantum channels between her and the three servers, while the quantum servers own quantum memory and have the ability to perform quantum computation. Assume that Alice has in mind the same quantum computation as that in the reviewed single-server and double-server BQC protocols. The detailed steps of the protocol are given in the following.

(T1) Let $\delta > 0$ be some fixed parameter. A trusted center prepares $n = (2+\delta)m$ Bell states in the form of $|\psi_{0,0}(B1_k,A_k)\rangle$ ($k = 1,2,\ldots,n$) and distributes the particle $B1_k$ of each Bell state to Bob1 and the other particle A_k to

Alice; similarly, the trusted center also generates another n Bell states in the form of $|\psi_{0,0}(B2_l, A'_l)\rangle$ $(l = 1,2,\ldots,n)$ and lets one particle $B2_l$ of each Bell state belong to Bob2 and the other particle A'_l belong to Alice.

(T2) For each particle A_k or A'_l arriving, Alice randomly chooses either to discard the particle or to transmit it to Bob3 and record the position of it. Bob3 restores the particles sent by Alice in quantum registers according to their incoming sequences.

(T3) There is a high probability that at least $2m$ particles are transmitted by Alice (if the protocol is not aborted). Suppose that m particles $A_{s_1}, A_{s_2}, \ldots, A_{s_m}$ and another m particles $A'_{t_1}, A'_{t_2}, \ldots, A'_{t_m}$, where $1 \leqslant s_1 < s_2 < \cdots < s_m \leqslant n$ and $1 \leqslant t_1 < t_2 < \cdots < t_m \leqslant n$, were chosen to be sent by Alice. In this step, Alice will ask Bob3 to perform Bell state measurements on particles A_{s_i} and A'_{t_i}, where $i \in \{1,2,\ldots,m\}$. When Alice wants Bob to measure particles A_{s_i} and A'_{t_i}, she tells Bob3 the positions of particles A_{s_i} and A'_{t_i} in the whole particles sequence that Bob3 received. Then Bob3 implements a Bell state measurement on the particles at these two positions and sends the measurement outcome $(z'_{s_i}, x'_{s_i}) \in \{0,1\}^2$ to Alice.

(T4) According to each measurement outcome (z'_{s_i}, x'_{s_i}), where $i \in \{1,2,\ldots,m\}$, Alice can know that the combined state of particles $B1_{s_i}$ and $B2_{t_i}$ is $|\psi_{z_{s_i},x_{s_i}}(B1_{s_i}, B2_{t_i})\rangle$ and obtain the values of z_{s_i} and x_{s_i}. For example, if the measurement outcome of particles A_{s_i} and A'_{t_i} is (0,0), the combined state of particles $B1_{s_i}$ and $B2_{t_i}$ is $|\psi_{0,0}(B1_{s_i}, B2_{t_i})\rangle$ based on Eq. (1) and the values of z_{s_i} and x_{s_i} are both equal to 0. At this moment, Bob1 and Bob2 share $\bigotimes_{i=1}^{m} |\psi_{z_{s_i},x_{s_i}}(B1_{s_i}, B2_{t_i})\rangle$ and other particles they hold are totally unrelated.

(T5) Alice sends Bob1 n classical messages $\{\tilde{\theta}_k = (-1)^{x_k}\theta_k + z_k\pi\}_{k=1}^{n}$, where $\theta_{s_1}, \theta_{s_2}, \ldots, \theta_{s_m}$ are randomly selected from the set S and useful for Alice's quantum computation, $(z_{s_1}, x_{s_1}), (z_{s_2}, x_{s_2}), \ldots, (z_{s_m}, x_{s_m})$ are determined by Alice at step T4, and when $k \in \{1,2,\ldots,n\} - \{s_1, s_2, \ldots, s_m\}$, $\theta_k \in S$ and $(z_k, x_k) \in \{0,1\}^2$ are chosen to let $\tilde{\theta}_1, \tilde{\theta}_2, \ldots, \tilde{\theta}_n$ be distributed as uniformly as possible over all the eight elements of the set S that is important for ensuring the security of the protocol and will be analyzed later. Note that it is significant to send Bob1 n classical messages rather than m classical messages since Bob1 cannot figure out which messages will really be used for Alice's quantum computation by doing so.

(T6) Bob1 performs a measurement on his particle $B1_k$ in the basis $\{\pm\tilde{\theta}_k\}$, where $k = 1,2,\ldots,n$. After measuring all the particles that Bob1 holds, he transmits the measurement outcomes $\{b_k\}_{k=1}^{n}$ to Alice. Alice just keeps $b_{s_1}, b_{s_2}, \ldots, b_{s_m}$.

(T7) Alice sends the classical information $\{t_i\}_{i=1}^{m}$ to Bob2 and asks him only to keep particles $B2_{t_1}, B2_{t_2}, \ldots, B2_{t_m}$. Bob2 does as Alice told and relabels these particles as $B2_1, B2_2, \ldots, B2_m$ in order. Note that the combined state of the m particles that Bob2 holds now is $\bigotimes_{i=1}^{m} |\theta_{s_i} + b_{s_i}\pi\rangle$.

(T8) Similar to D5, Alice starts the reviewed single-server BQC protocol with Bob2 from step S2, replacing θ_i with $\theta_{s_i} + b_{s_i}\pi$ $(i = 1,2,\ldots,m)$.

In the following, we will show that the proposed triple-server BQC protocol is as secure as the reviewed double-server BQC protocol if the three servers do not communicate with each other and it is also secure even if the three servers communicate mutually except that in some special cases, partial information of Alice will leak to the Bobs.

Suppose three servers Bob1, Bob2, and Bob3 do not communicate mutually. First, for the server Bob3, he actually does not implement the real quantum computation that Alice wants. What Bob3 does is that he just helps Alice implement Bell state measurements to let Bob1 and Bob2 share Bell states. So after the Bell state measurements performed by Bob3, the protocol can be reduced to a double-server BQC protocol. Second, for the server Bob1, the information he received is n classical messages $\{\tilde{\theta}_k\}_{k=1}^{n}$ and then Bob1 can get n measurement results $\{b_k\}_{k=1}^{n}$, while the number of these information in the reviewed double-server BQC protocol is m. However, in fact, only m classical messages $\tilde{\theta}_{s_1}, \tilde{\theta}_{s_1}, \ldots, \tilde{\theta}_{s_m}$ and m measurement results $b_{s_1}, b_{s_1}, \ldots, b_{s_m}$ are used for the quantum computation. Thus, the proposed protocol is secure against Bob1 as that in the reviewed double-server BQC protocol. Third, for the server Bob2, he knows which particles are employed for the quantum computation and receives the information $\{\delta_i\}_{i=1}^{m}$ from Alice, which are the same as that in the reviewed double-server BQC protocol. Thus, the proposed protocol is secure against Bob2 as that in the reviewed double-server BQC protocol.

If Bob1, Bob2, and Bob3 can communicate with each other they may cooperate and attempt to obtain the information related to Alice's quantum computation, such as something about $\{\theta_{s_i}\}_{i=1}^{m}$ or $\{\phi_i\}_{i=1}^{m}$. Assume that Bob1 who knows $\{\tilde{\theta}_k = (-1)^{x_k}\theta_k + z_k\pi\}_{k=1}^{n}$ and $\{b_k\}_{k=1}^{n}$ is chosen to do such thing. Then Bob2 tells his information $\{\delta_i = (\theta_{s_i} + b_{s_i}\pi + \phi'_i + r_i\pi) \bmod 2\pi\}_{i=1}^{m}$ and $\{t_i\}_{i=1}^{m}$ to Bob1. Similarly, Bob3 reveals the Bell state measurement outcomes $\{z'_{s_i}, x'_{s_i}\}_{i=1}^{m}$ to Bob1. If the values of all n classical messages $\{\tilde{\theta}_k\}_{k=1}^{n}$ are distributed uniformly on the eight elements of the set S, based on all the information that Bob1 obtained, he still cannot learn anything about $\{\theta_{s_i}\}_{i=1}^{m}$ or $\{\phi_i\}_{i=1}^{m}$ since he does not know the values of $\{s_i\}_{i=1}^{m}$ which are randomly chosen by Alice. For instance, from Bob3's information $\{z'_{s_i}, x'_{s_i}\}_{i=1}^{m}$, Bob1 can learn the values of $\{z_{s_i}, x_{s_i}\}_{i=1}^{m}$, but without the knowledge of $\{s_i\}_{i=1}^{m}$, he still cannot figure out the values of $\{\theta_{s_i}\}_{i=1}^{m}$ even though he knows $\{\tilde{\theta}_k\}_{k=1}^{n}$; similarly, from Bob2's information $\{\delta_i\}_{i=1}^{m}$ and $\{t_i\}_{i=1}^{m}$, Bob1 also cannot obtain any information about $\{\phi_i\}_{i=1}^{m}$ without knowing $\{\theta_{s_i} + b_{s_i}\pi\}_{i=1}^{m}$. However, if all the values of $\{\tilde{\theta}_k\}_{k=1}^{n}$ are not distributed uniformly over all the elements of the set S, especially when they do not cover all eight possibilities, Bob1 may get partial information about Alice's $\{\theta_{s_i}\}_{i=1}^{m}$ or $\{\phi_i\}_{i=1}^{m}$ using the following method. Bob1 has all the angles $\{\tilde{\theta}_k\}_{k=1}^{n}$ and later he learns the value of each pair $\{z_{s_i}, x_{s_i}\}$ $(i = 1,2,\ldots,m)$ from Bob3; then Bob1 obtains the set S_i (i varies from 1 to m) by computing $\{(-1)^{x_{s_i}}(\tilde{\theta}_1 - z_{s_i}\pi), (-1)^{x_{s_i}}(\tilde{\theta}_2 - z_{s_i}\pi), \ldots, (-1)^{x_{s_i}}(\tilde{\theta}_n - z_{s_i}\pi)\}$. So Bob1 can learn that the elements of S_i will be distributed unequally or take fewer than eight possibilities and then the possible outcomes of Alice's θ_{s_i} will also occur unequally or take fewer than eight possibilities (note that if the size of n is less than eight, the choices of θ_{s_i} are certainly fewer than eight possibilities), while before the protocol, Bob1 knows θ_{s_i} has eight possibilities in the same probability. Hence, Bob1's information about Alice's θ_{s_i} is increased. For example, suppose Alice sends Bob four classical messages $\tilde{\theta}_1 = 0$, $\tilde{\theta}_2 = \pi/2$, $\tilde{\theta}_3 = \pi$, and $\tilde{\theta}_4 = 0$.

Later, Bob1 learns $z_{s_1} = 0$ and $x_{s_1} = 0$ from Bob3. Then Bob1 can know that θ_{s_1} has three possible values 0, $\pi/2$, and π and the probabilities of them are $1/2$, $1/4$, and $1/4$, respectively. However, before the protocol, Bob1 knows that θ_{s_1} will take eight possibilities with equal probability. Obviously, the entropy of θ_{s_1} is decreased from $\log 8$ to $\log \sqrt{8}$ and thus Bob1's knowledge about Alice's computation information θ_{s_1} is increased after the protocol. Similarly, after Bob1 learns something about $\{\theta_{s_i}\}_{i=1}^m$ and obtains $\{\delta_i\}_{i=1}^m$ from Bob2, he also can learn some information about ϕ_i by computing $\delta_i - \theta_{s_i}$ (i varies from 1 to m). Therefore, the communication among the three quantum servers does not affect the security of the proposed triple-server BQC protocol except for the cases when the values of $\{\tilde{\theta}_k\}_{k=1}^n$ are not distributed uniformly over all the elements of the set S or have fewer than eight possibilities.

In conclusion, we have proposed a triple-server BQC protocol in which the almost classical client who does not require any quantum computational power or quantum resources and only needs to be able to receive or send qubits can delegate quantum computation to three servers, while still keeping one's input, output, and procedure private. In particular, we have shown that the mutual communication among the three servers will not affect the security of the proposed triple-server BQC protocol except for some special cases. Actually, it is more practicable to allow powerful quantum servers to communicate with each other.

However, we have not dealt with the problem of entanglement distillation and thus the trusted center has to distribute high-fidelity Bell states between the participants, which is a tough task. Morimae and Fujii ingeniously make entanglement distillation possible when the quantum servers are noncommunicating. So it is natural to ask whether entanglement distillation is possible when the quantum servers do not know which particles are in combined Bell states. This is an interesting question that deserves further study.

We would like to thank the anonymous referee for helpful comments. This work was sponsored by the Natural Science Foundation of China (Grants No. 61202398, No. 61391240194, No. 61272295, and No. 61100216). The work of C. Wu was supported by the Foundation for Distinguished Young Talents in Higher Education of Guangdong (Grant No. LYM11093).

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).
[2] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
[3] P. W. Shor, *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, 1994), pp. 124–134.
[4] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[5] T. Morimae and K. Fujii, Phys. Rev. A **87**, 050301(R) (2013).
[6] A. M. Childs, Quantum Inf. Comput. **5**, 456 (2005).
[7] P. Arrighi and L. Salvail, Int. J. Quantum Inf. **04**, 883 (2006).
[8] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, 2009), pp. 517–526.
[9] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
[10] D. Aharonov, M. Ben-Or, and E. Eban, *Proceedings of the First Symposium on Innovations in Computer Science* (Tsinghua University Press, Beijing, 2010), pp. 453–469.
[11] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).
[12] T. Morimae and K. Fujii, Nat. Commun. **3**, 1036 (2012).
[13] T. Morimae, Phys. Rev. Lett. **109**, 230502 (2012).
[14] J. F. Fitzsimons and E. Kashefi, arXiv:1203.5217.
[15] T. Sueki, T. Koshiba, and T. Morimae, Phys. Rev. A **87**, 060301(R) (2013).
[16] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Phys. Rev. Lett. **111**, 230501 (2013).
[17] A. Mantri, C. A. Perez-Delgado, and J. F. Fitzsimons, Phys. Rev. Lett. **111**, 230502 (2013).
[18] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, arXiv:1301.3662.
[19] T. Morimae and T. Koshiba, arXiv:1306.2113.
[20] T. Morimae and K. Fujii, Phys. Rev. Lett. **111**, 020502 (2013).
[21] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[22] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
[23] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).
[24] R. E. S. Polkinghorne and T. C. Ralph, Phys. Rev. Lett. **83**, 2095 (1999).
[25] X. Ma, S. Zotter, J. Kofler, R. Ursin, T. Jennewein, Č. Brukner, and A. Zeilinger, Nat. Phys. **8**, 479 (2012).
[26] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[27] H. Lu and G. Guo, Phys. Lett. A **276**, 209 (2000).
[28] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[29] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).
[30] Z. J. Zhang and Z. X. Man, Phys. Rev. A **72**, 022303 (2005).
[31] X. M. Xiu, H. K. Dong, L. Dong, Y. J. Gao, and F. Chi, Opt. Commun. **282**, 2457 (2009).
[32] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).