Secure Entanglement Distillation for Double-Server Blind Quantum Computation

Tomoyuki Morimae[1,2,*] and Keisuke Fujii[3,4,5,†]

[1]ASRLD Unit, Gunma University, 1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan
[2]Department of Physics, Imperial College London, London SW7 2AZ, United Kingdom
[3]The Hakubi Center for Advanced Research, Kyoto University, Yoshida-Ushinomiya-cho, Sakyo-ku, Kyoto 606-8302, Japan
[4]Graduate School of Informatics, Kyoto University, Yoshida Honmachi, Sakyo-ku, Kyoto 606-8501, Japan
[5]Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan
(Received 29 April 2013; published 9 July 2013)

Blind quantum computation is a new secure quantum computing protocol where a client, who does not have enough quantum technologies at her disposal, can delegate her quantum computation to a server, who has a fully fledged quantum computer, in such a way that the server cannot learn anything about the client's input, output, and program. If the client interacts with only a single server, the client has to have some minimum quantum power, such as the ability of emitting randomly rotated single-qubit states or the ability of measuring states. If the client interacts with two servers who share Bell pairs but cannot communicate with each other, the client can be completely classical. For such a double-server scheme, two servers have to share clean Bell pairs, and therefore the entanglement distillation is necessary in a realistic noisy environment. In this Letter, we show that it is possible to perform entanglement distillation in the double-server scheme without degrading the security of blind quantum computing.

DOI: 10.1103/PhysRevLett.111.020502 PACS numbers: 03.67.−a

A first generation quantum computer will be implemented in a "cloud" style, since only a limited number of groups, such as huge industries and governments, will be able to possess it. When a client uses such a quantum server via remote access, it is crucial to protect the client's privacy. Blind quantum computation [1–12] is a new secure quantum computing protocol which can guarantee the security of a client's privacy in such cloud quantum computing. Protocols of blind quantum computation enable a client (Alice), who does not have enough quantum technologies at her disposal, to delegate her quantum computation to a server (Bob), who has a fully fledged quantum computer, in such a way that Alice's input, output, and program are hidden from Bob [1–12].

The original protocol of blind quantum computation was proposed by Broadbent, Fitzsimons, and Kashefi (BFK) [1]. Their protocol uses measurement-based quantum computation on the cluster state (graph state) by Raussendorf and Briegel [13]. A proof-of-principle experiment of the BFK protocol has also been achieved recently with a quantum optical system [3]. The BFK protocol has recently been generalized to other blind quantum computing protocols which use measurement-based quantum computation on the Affleck-Kennedy-Lieb-Tasaki state [5,14,15], continuous-variable measurement-based quantum computation [7,16], and the ancilla-driven model [10,17].

Since the original BFK protocol was proposed, new protocols have been developed in order for blind quantum computation to be more practical. One direction is making blind protocols more fault tolerant. While the BFK protocol, which utilizes the brickwork state, would be fault tolerant, its threshold value is extremely small. The recently proposed topological blind quantum computation [6] employs a special three-dimensional cluster state [18] and allows us to perform topologically protected blind quantum computation even with a high error probability of 0.43% (i.e., fidelity of 99.57%) in preparations, measurements, and gate operations.

Another direction is making Alice as classical as possible. In the above BFK-based protocols, Alice emits randomly rotated single-qubit states, such as single-photon states. Recently, it was shown [4] that instead of single-photon states, coherent states are also sufficient. Since coherent states are considered to be more classical than single-photon states, this result suggests that Alice can be more classical.

It is also possible to make Alice completely classical: the double-sever blind protocol was introduced in Ref. [1], where two Bobs share Bell pairs (but cannot perform classical communication with each other) and perform computational tasks ordered by Alice's classical message. The double-server blind protocol is also fault tolerant, but Bell pairs of fidelity above 99% are required even if topological blind quantum computation is employed. Since Bell pairs have to be sent from the third party or Alice herself via public quantum channels, such an ability to generate high-fidelity Bell pairs or encoding them into quantum error correction codes would be too demanding.

In this Letter, we settle this problem. We show that it is possible to perform entanglement distillation in the double-server scheme without degrading the security of blind quantum computing. As a result, the required fidelity of the Bell pairs is improved dramatically to 81%, which is determined by the hashing bound and achieved by quantum random coding [19,20]. Since the Bell pair generation of fidelity higher than 81% is nowadays easily achievable by using, for example, parametric down-conversion, the present result is crucial in blind quantum computation to make Alice (or the third party) as classical as possible by using practically noisy Bell pair sources and quantum channels.

Before proceeding to our main result, let us briefly review the BFK blind protocol [1]. Assume that Alice wants to perform measurement-based quantum computation on the m-qubit graph state corresponding to the graph G. The quantum algorithm which Alice wants to run is specified with the measurement basis $\{|0\rangle \pm e^{i\phi_j}|1\rangle\}$ for the jth qubit ($j=1,2,\ldots,m$), where $\phi_j \in \{(k\pi)/4|k=0,1,\ldots,7\}$. (Note that such $X-Y$ plane measurements are universal [13].) The BFK protocol runs as follows (see also Fig. 1). (S1) Alice tells Bob the graph G [21]. (S2) Alice sends Bob $\bigotimes_{j=1}^m|\theta_j\rangle$, where $|\theta_j\rangle \equiv |0\rangle + e^{i\theta_j}|1\rangle$ and θ_j is randomly chosen by Alice from $\{(k\pi)/4|k=0,1,\ldots,7\}$. (S3) Bob makes $|G\{\theta_j\}\rangle \equiv (\bigotimes_{(i,j)\in E} CZ_{i,j})\bigotimes_{j=1}^m|\theta_j\rangle$, where E is the set of edges of G and $CZ_{i,j}$ is the CZ gate between the ith and jth qubits. (S4) Alice and Bob now perform measurement-based quantum computation on $|G\{\theta_j\}\rangle$ with two-way classical communications as follows: when Alice wants Bob to measure the jth qubit ($j=1,2,\ldots,m$) of $|G\{\theta_j\}\rangle$, she sends Bob $\delta_j \equiv \theta_j + \phi'_j + r_j\pi$, where $r_j \in \{0,1\}$ is a random binary chosen by Alice and ϕ'_j is the modified version of ϕ_j according to the previous measurement results, which is the standard feed forwarding of the one-way model [13]. Bob measures the jth qubit in the basis $\{|0\rangle \pm e^{i\delta_j}|1\rangle\}$ and tells the measurement result to Alice.

We call this protocol the single-server protocol, since there is only a single server (Bob). It was shown [1] that whatever Bob does, he cannot learn anything about Alice's input, output, or algorithm.

In the above single-server protocol, Alice has to have the ability of emitting randomly rotated single-qubit states $\{|\theta_j\rangle\}_{j=1}^m$. It was shown in Ref. [1] that if we have two servers (Bob1 and Bob2) who share Bell pairs but cannot communicate with each other, Alice can be completely classical. (Alice only has to have a classical computer and two classical channels; one is between Alice and Bob1, and the other is between Alice and Bob2.) We call such a scheme the double-server scheme, since there are two servers. A protocol of the double-server scheme runs as follows [1] (see also Fig. 2). (D1) A trusted center distributes Bell pairs to Bob1 and Bob2 [22]. Now, Bob1 and Bob2 share m Bell pairs $(|00\rangle + |11\rangle)^{\otimes m}$. (D2) Alice sends Bob1 classical messages $\{\theta_j\}_{j=1}^m$, where θ_j is randomly chosen by Alice from $\{(k\pi)/4|k=0,1,\ldots,7\}$. (D3) Bob1 measures his qubit of the jth Bell pair in the basis $\{|0\rangle \pm e^{-i\theta_j}|1\rangle\}$ ($j=1,\ldots,m$). Bob1 tells Alice the measurement results $\{b_j\}_{j=1}^m \in \{0,1\}^m$. (D4) After these Bob1 measurements, Bob2 has $\bigotimes_{j=1}^m Z_j^{b_j}|\theta_j\rangle = \bigotimes_{j=1}^m|\theta_j + b_j\pi\rangle$. Now, Alice and Bob2 can start the single-server BFK protocol with the modification $\{\theta_j\}_{j=1}^m \to \{\theta_j + b_j\pi\}_{j=1}^m$.

In addition to the advantage of the completely classical Alice, the double-server scheme is intensively studied in computer science in the context of the multiprover interactive proof system, which assumes computationally unbounded and untrusted prover (server), and in device-independent quantum key distribution [1,23,24].

Note that the impossibility of the communication between two Bobs is crucial in the double-server protocol. If Bob1 can send some messages to Bob2, Bob1 can tell Bob2 $\{\theta_j + b_j\pi\}_{j=1}^m$, and then Bob2 can learn something about $\{\phi_j\}_{j=1}^m$, since Bob2 knows $\{\theta_j + b_j\pi + \phi'_j + r_j\pi\}_{j=1}^m$. On the other hand, if Bob2 can tell Bob1 $\{\theta_j + b_j\pi + \phi'_j + r_j\pi\}_{j=1}^m$, Bob1 can learn something about $\{\phi_j\}_{j=1}^m$, since Bob1 knows $\{\theta_j + b_j\pi\}_{j=1}^m$. In these cases, the security of Alice's privacy is no longer guaranteed.

In order to perform the correct double-server protocol, two Bobs must share clean Bell pairs. Sharing clean Bell pairs is also crucial in many other quantum information protocols such as quantum teleportation [25], quantum key distribution [26,27], and distributed quantum computation

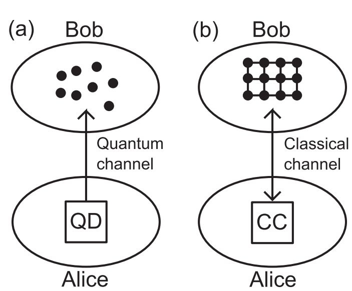

FIG. 1. The single-server blind protocol. (a) Alice sends many single-qubit states to Bob. QD is a device which emits randomly rotated single qubits. (b) Bob creates a resource state. Alice and Bob perform measurement-based quantum computation through the two-way classical channel. CC is a classical computer.

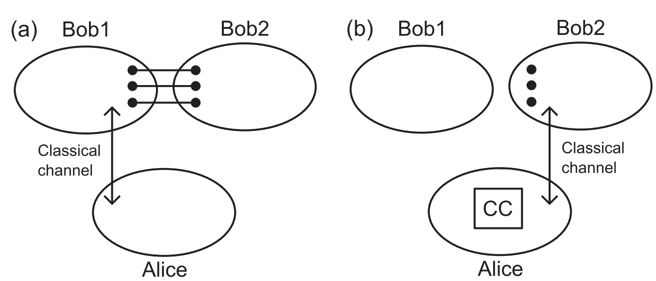

FIG. 2. The double-server blind protocol. (a) Bob1 and Bob2 share Bell pairs. Alice sends classical messages to Bob1. Bob1 performs measurements on his qubits of the Bell pairs and tells the measurement results to Alice. (b) Alice and Bob2 run the single-server blind protocol through the two-way classical channel. CC is a classical computer.

[28–32]. One standard way of sharing clean Bell pairs in a noisy environment is entanglement distillation [19,20,33,34]. In entanglement distillation protocols, two people, say, Bob1 and Bob2, who want to share clean Bell pairs, start with some dirty n Bell pairs. Then, they perform local operations with some classical communications and finally "distill" m ($m < n$) clean Bell pairs [19,20,33,34].

If we consider the application of entanglement distillation to the double-server blind protocol, one huge obstacle is that two Bobs are not allowed to communicate with each other in the double-server scheme. Hence, message exchanges between two Bobs, which are necessary for entanglement distillation, must be done through Alice's mediation; i.e., Bob1 (Bob2) sends a message to Alice, and Alice transfers it to Bob2 (Bob1). It is not self-evident that the security of the double-server blind protocol is guaranteed even if we plug an entanglement distillation protocol into the double-server blind protocol [35]. For example, Bob1 might send a message to Alice pretending that it is a "legal" message for entanglement distillation. Alice might naively forward that message to Bob2 without noticing Bob1's evil intention and believing that it is a harmless message. In this case, Bob1 can indirectly send a message to Bob2, and hence the security of the double-server protocol is no longer guaranteed.

If the entire entanglement distillation is completed before starting the double-server protocol, and if Alice only delegates her computation to the Bobs once, then the communication between two Bobs during the entanglement distillation is harmless, since when they are doing the entanglement distillation, messages related to Alice's computation are not yet sent to the Bobs. However, if Alice delegates more than twice, then two Bobs might exchange information about the previous double-server computation during entanglement distillation for the next round of computation as in the case of the "device-independence" argument of the quantum key distribution with devices that have memory [36]. Furthermore, entanglement distillation might be done in parallel with the double-server protocol in order to avoid decoherence. In these cases, we must be careful about the communication between two Bobs during entanglement distillation. In terms of the composable security, this means that we are interested in the composable security of the "distillation + blind computing" protocol [35].

Throughout this Letter, we denote four Bell states by $|\psi_{z,x}\rangle \equiv (I \otimes X^x Z^z)(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$, where $(z, x) \in \{0,1\}^2$ and $X \equiv |0\rangle\langle 1| + |1\rangle\langle 0|$.

Protocol.—Now, let us show that entanglement distillation by two Bobs is indeed possible without degrading the security. As in the case of the original BFK double-server protocol, a trusted center (or Alice) generates n Bell states $|\psi_{00}\rangle^{\otimes n}$ and distributes them to two Bobs; one qubit of each $|\psi_{00}\rangle$ is sent to Bob1 and the other to Bob2. Because of the noise in the channel between the center and the Bobs, each Bell state decoheres $|\psi_{00}\rangle \to \rho$. Hence, two Bobs share n impure pairs $\rho^{\otimes n}$, where ρ is a dirty Bell state: one qubit of ρ is possessed by Bob1 and the other by Bob2. Without loss of generality, we can assume that ρ is the Werner state $\rho = F\psi_{11} + (1-F)/3(\psi_{00} + \psi_{01} + \psi_{10})$, where $\psi \equiv |\psi\rangle\langle\psi|$. If it is not the Werner state, it can be converted into the Werner state by using the twirling operation (after applying $I \otimes XZ$) [20]. In order to perform the twirling operation, Alice only has to randomly choose a $SU(2)$ operator and tell its classical description to two Bobs. Therefore, the twirling operation does not affect the security.

Since ρ is Bell diagonal, $\rho^{\otimes n}$ is the mixture of tensor products of Bell states:

$$\rho^{\otimes n} = \sum_{(z_1,x_1,\ldots,z_n,x_n)\in\{0,1\}^{2n}} p(z_1, x_1, \ldots, z_n, x_n) \bigotimes_{j=1}^{n} \psi_{z_j,x_j}.$$

Alice randomly chooses a $2n$-bit string s_1 and sends it to two Bobs. This s_1 is chosen completely randomly, being independent of other parameters (such as θ_j, ϕ_j, etc.). Each Bob then performs a certain local unitary operation which is determined by s_1. Each Bob next measures a qubit of a single pair in the computational basis and tells the measurement result to Alice. [The detail of the unitary operation, which is irrelevant here, is given in Ref. [20]. Which pair is measured is also determined by s_1 [20]. In brief, these unitary operations and measurements are performed for obtaining $s_1 \cdot v$ (mod2) for the hashing, where $v \equiv (z_1, x_1, \ldots, z_n, x_n)$.] From these measurement results by the Bobs, Alice can gain a single bit $s_1 \cdot v$ (mod2) of information.

Since a single pair is measured out, now two Bobs share $n-1$ pairs. If Alice and two Bobs repeat a similar procedure [i.e., Alice randomly chooses a $2(n-1)$-bit string s_2 and tells it to two Bobs, and then two Bobs perform local operations, measure a single pair in the computational basis, and tell the measurement results to Alice], Alice can gain another single bit of information. In this way, they repeat this procedure many times, and Alice obtains enough bits to perform the hashing, which works as follows.

The probability distribution $p(z_1, x_1, \ldots, z_n, x_n)$ has almost all its weight for a set of $\sim 2^{nS(\rho)}$ "likely" strings, where $S(\rho)$ is the von Neumann entropy of ρ. The probability that a $2n$-bit string $(z_1, x_1, \ldots, z_n, x_n)$ falls outside of the set of the $2^{n[S(\rho)+\epsilon]}$ most probable strings is $O(e^{-\epsilon^2 n})$ [20]. Therefore, Alice can (almost) specify $p(z_1, x_1, \ldots, z_n, x_n)$ if she gains $nS(\rho)$ bits of information about $p(z_1, x_1, \ldots, z_n, x_n)$. This means that it is sufficient for Alice and two Bobs to repeat the above procedure for $nS(\rho)$ times. Then, two Bobs spend $nS(\rho)$ pairs for measurements, and therefore at the end of the distillation, they share $m \equiv n - nS(\rho)$ pairs $\bigotimes_{j=1}^{m} |\psi_{z_j,x_j}\rangle$, where $(z_j, x_j) \in \{0,1\}^2$. Alice knows the $2m$-bit string $(z_1, x_1, \ldots, z_m, x_m)$.

After the distillation, Alice and two Bobs can start the double-server protocol. Now, we modify the double-server protocol as follows. (D1′) Two Bobs share $\bigotimes_{j=1}^{m}|\psi_{z_j,x_j}\rangle$. (D2′) Alice sends Bob1 classical messages $\{\theta_j' \equiv (-1)^{x_j}\theta_j + z_j\pi\}_{j=1}^{m}$, where θ_j is randomly chosen by Alice from $\{(k\pi)/4|k=0,1,\ldots,7\}$. (D3′) Bob1 measures his qubit of the jth Bell pair in the basis $\{|0\rangle \pm e^{-i\theta_j'}|1\rangle\}$ ($j=1,\ldots,m$). Bob1 tells Alice the measurement results $\{b_j\}_{j=1}^{m} \in \{0,1\}^m$. (D4′) The same as D4. Since D4′ is the same as D4, it is obvious that Alice can run the correct single-server blind quantum computation with Bob2.

Bob1 cannot send any messages to Bob2.—Let us show that Bob1 cannot send any messages to Bob2. What Bob2 receives from Alice are bit strings $s_1,\ldots,s_{n-m}$ and $\{\theta_j + b_j\pi + \phi_j' + r_j\pi\}_{j=1}^{m}$. Since $s_1,\ldots,s_{n-m}$ are completely uncorrelated with what Bob1 sends to Alice, Bob2 cannot gain any information about Bob1's message from $s_1,\ldots,s_{n-m}$. Furthermore, r_j is randomly taken by Alice from $\{0,1\}$, being independent of what Bob1 sends to Alice. Therefore, Bob2 cannot gain any information about b_j from $\theta_j + b_j\pi + \phi_j' + r_j\pi$. Bob1 and Bob2 share entangled pairs. However, due to the no-signaling principle, only sharing entangled pairs is useless for message transmission. Hence, Bob1 cannot send any messages to Bob2.

Bob2 cannot send any messages to Bob1.—Next, let us show that Bob2 cannot send any messages to Bob1. What Bob1 receives from Alice are bit strings $s_1,\ldots,s_{n-m}$ and $\{\theta_j' \equiv (-1)^{x_j}\theta_j + z_j\pi\}_{j=1}^{m}$. Again, $s_1,\ldots,s_{n-m}$ are useless for the message transmission from Bob2 to Bob1. Furthermore, θ_j is randomly chosen by Alice from $\{(k\pi)/4|k=0,1,\ldots,7\}$, being independent of what Bob2 sends to Alice and $(z_1,x_1,\ldots,z_m,x_m)$. Therefore, Bob1 cannot gain any information about Bob2's message from θ_j'. Hence, Bob2 cannot send any message to Bob1.

The two Bobs cannot learn Alice's computational information.—Finally, let us show the security of Alice's computational information. First, from Bob2's viewpoint, the difference between our protocol (i.e., the distillation plus the modified double-server protocol) and the original BFK double-server protocol is only that Bob2 receives bit strings $s_1,\ldots,s_{n-m}$ from Alice. Since these bit strings are completely uncorrelated with Alice's computational information, our protocol is as secure as the original BFK double-server protocol against Bob2.

Second, from Bob1's viewpoint, the differences between our protocol and the original BFK double-server protocol are that (i) Bob1 receives bit strings $s_1,\ldots,s_{n-m}$ from Alice. (ii) Bob1 receives $\theta_j' \equiv (-1)^{x_j}\theta_j + z_j\pi$ instead of θ_j from Alice ($j=1,2,\ldots,m$). Again, we can safely ignore (i). Regarding (ii): since θ_j is randomly taken from $\{(k\pi)/4|k=0,1,\ldots,7\}$, being independent of Alice's computational information and $(z_1,x_1,\ldots,z_m,x_m)$, Bob1 cannot gain any information about Alice's computation from θ_j'. Hence, our protocol is as secure as the original double-server BFK protocol against Bob1.

T. M. was supported by JSPS and the Program to Disseminate Tenure Tracking System by MEXT. K. F. was supported by the MEXT Grant-in-Aid for Scientific Research on Innovative Areas No. 20104003.

*morimae@gunma-u.ac.jp
†keisukejayorz@gmail.com

[1] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Proceedings of the 50th Annual IEEE Symposium on the Foundations of Computer Science* (IEEE, New York, 2009), p. 517.
[2] J. Fitzsimons and E. Kashefi, arXiv:1203.5217.
[3] S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
[4] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).
[5] T. Morimae, V. Dunjko, and E. Kashefi, arXiv:1009.3486.
[6] T. Morimae and K. Fujii, Nat. Commun. **3**, 1036 (2012).
[7] T. Morimae, Phys. Rev. Lett. **109**, 230502 (2012).
[8] T. Morimae, arXiv:1208.1495.
[9] T. Morimae and K. Fujii, Phys. Rev. A **87**, 050301(R) (2013).
[10] T. Sueki, T. Koshiba, and T. Morimae, Phys. Rev. A **87**, 060301(R) (2013).
[11] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, arXiv:1301.3662.
[12] T. Morimae and T. Koshiba, arXiv:1306.2113.
[13] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[14] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki, Commun. Math. Phys. **115**, 477 (1988).
[15] G. K. Brennen and A. Miyake, Phys. Rev. Lett. **101**, 010502 (2008).
[16] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Phys. Rev. Lett. **97**, 110501 (2006).
[17] J. Anders, D. K. L. Oi, E. Kashefi, D. E. Browne, and E. Andersson, Phys. Rev. A **82**, 020301(R) (2010).
[18] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007).
[19] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[20] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[21] One might think that Bob can gain some information about Alice's computation from graph G. However, there are several ways of hiding Alice's true graph from Bob [1,2,6]. One idea is to use the so-called brickwork state, which is a graph state with a specific graph where universal quantum computation can be done with only $X-Y$ plane measurements [1].
[22] Since two Bobs cannot communicate with each other, it is impossible for one Bob to generate a Bell pair and send half of it to the other Bob.

[23] D. Aharonov, M. Ben-Or, and E. Eban, *Proceedings of Innovation in Computer Science 2010 (ICS 2010)*, (Tsinghua University Press, Beijing, China, 2010), p. 453.
[24] B. W. Reichardt, F. Unger, and U. Vazirani, arXiv:1209.0448.
[25] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[26] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984).
[27] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[28] K. Fujii, T. Yamamoto, M. Koashi, and N. Imoto, arXiv:1202.6588.
[29] Y. Li and S.C. Benjamin, New J. Phys. **14**, 093008 (2012).
[30] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Phys. Rev. A **59**, 4249 (1999).
[31] W. Dür and H. J. Briegel, Phys. Rev. Lett. **90**, 067901 (2003).
[32] L. Jiang, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. A **76**, 062323 (2007).
[33] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[34] W. Dür and H. J. Briegel, Rep. Prog. Phys. **70**, 1381 (2007).
[35] Do not misunderstand that this suggests that existing blind protocols without distillation are insecure: the stand-alone and composable securities of blind protocols themselves are already established [1,2,4–6,8,9,11,12].
[36] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. Lett. **110**, 010503 (2013).