PHYSICAL REVIEW A **87**, 060301(R) (2013)

Ancilla-driven universal blind quantum computation

Takahiro Sueki,[1] Takeshi Koshiba,[1] and Tomoyuki Morimae[2,3]

[1]*Graduate School of Science and Engineering, Saitama University, 255 Shimo-Okubo, Sakura, Saitama 338-8570, Japan*

[2]*Department of Physics, Imperial College London, London SW7 2AZ, United Kingdom*

[3]*ASRLD Unit, Gunma University, 1-5-1 Tenjin-cho, Kiryu-shi, Gunma 376-0052, Japan*

(Received 27 October 2012; revised manuscript received 1 April 2013; published 6 June 2013)

Blind quantum computation is a new quantum secure protocol, which enables Alice who does not have enough quantum technology to delegate her computation to Bob who has a fully fledged quantum power without revealing her input, output, and algorithm. So far, blind quantum computation has been considered only for the circuit model and the measurement-based model. Here we consider the possibility and the limitation of blind quantum computation in the ancilla-driven model, which is a hybrid of the circuit and the measurement-based models.

DOI: 10.1103/PhysRevA.87.060301 PACS number(s): 03.67.Lx, 03.67.Dd, 03.65.Ud

I. INTRODUCTION

Traditionally, quantum computation has been studied in the circuit model [1], where the quantum register which stores quantum information consists of many qubits, and a quantum gate operation is performed by directly accessing one or two qubits in the quantum register. Another canonical model of quantum computation is the one-way model [2] (or more general measurement-based models [3–13]), where the universal quantum computation is performed by adaptive local measurements on a highly entangled resource state. Recently, a mixture of those two models, which is called the ancilla-driven quantum computation, was proposed [14,15]. In this model, the quantum register is a set of many qubits like the circuit model, whereas a quantum gate operation is, like the one-way model, performed by adaptive local measurements: one or two register qubits are coupled to a single mobile ancilla, and the ancilla is measured after establishing the interaction between the ancilla and register qubit(s). The back action of this measurement provides the desired gate operation, such as a single qubit rotation or an entangling 2-qubit operation, on register qubit(s). In the ancilla-driven model, the universal quantum computation is performed with only a single type of interaction [controlled Z (CZ) or SWAP + CZ] between the ancilla and register qubit(s). It is a great advantage for experiments, since in many experimental setups, implementing various different types of interactions at the same time is very difficult (such as the solid-based quantum computation). Furthermore, the roles of the register and the information carrier are clearly separated, and no direct action on the register is required. Therefore, it is also useful in experimental systems where measurements destroy quantum states, such as photonic systems. In short, this model is a natural theoretical model of the "hybrid quantum computer" where the flying ancilla mediates interactions between static qubits (such as the chip-based quantum computation [16,17] or the hybrid system of matter and optical elements [18,19]).

In the future, when a scalable quantum computer is realized, quantum computation should be done in the "cloud" style, since only a limited number of people would have enough money and technology to create and maintain quantum computers. Blind quantum computation [20–29] ensures the privacy of the client in such a cloud quantum computing. In protocols of blind quantum computation, Alice, the client, does not have enough quantum technology. On the other hand, Bob, the server, has a fully fledged quantum power. Alice asks Bob to perform her computation on his quantum computer in such a way that Bob cannot learn anything about her input, output, or algorithm. Blind quantum computation was initially considered by using the circuit model [20–22]. However, in that case, Alice needs a quantum memory. Recent new ideas of blind quantum computation which use measurement-based models have succeeded to exempt Alice from a quantum memory [23–29].

In terms of the computational power, measurement-based models do not offer any advantage over the circuit model, since the circuit model can be simulated by measurement-based models and vice versa. However, measurement-based models have provided new points of view for studying quantum computation, and in fact such new viewpoints have enabled plenty of successes which have never been done in the circuit model, such as high-threshold fault tolerance [10–12,30–36], clarification of the roles of entanglement played in quantum computation [3,37–40], and relations to condensed-matter physics [3–7,13,41–44]. Therefore it is important to explore the possibility of blind quantum computation on models other than the circuit model and measurement-based models.

II. ANCILLA-DRIVEN QUANTUM COMPUTATION

We first define several notations for the basis and for the basic transformations as follows: $|+_{\theta,\varphi}\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\varphi}\sin(\frac{\theta}{2})|1\rangle$, $|-_{\theta,\varphi}\rangle = \sin(\frac{\theta}{2})|0\rangle - e^{i\varphi}\cos(\frac{\theta}{2})|1\rangle$, $R_x(\theta) = e^{-\frac{i\theta X}{2}}$ and $R_z(\theta) = e^{-\frac{i\theta Z}{2}}$. We conventionally use the notations $\{|\pm\rangle\}$ and $\{|0\rangle,|1\rangle\}$ to denote the bases along X and Z axes in the Bloch sphere, respectively. Measurement outcome is represented by $s \in \{0,1\}$, associated with ±. We denote the ith measurement outcome by s_i.

We review the ancilla-driven quantum computation (ADQC) proposed in [14,15]. ADQC is performed with a 1-qubit ancilla, only on which we can make measurements, and (a single or a few) 2-qubit entangle operator(s) $\tilde{E}_{as}$. As in Fig. 1(a), $\tilde{E}_{as}$ can be decomposed into $\tilde{E}_{as} = (W_s \otimes W'_a)D_{as}(V_s \otimes V'_a)$ by the Cartan decomposition [45], where V_s, V'_a, W_s, and W'_a are 1-qubit local unitaries and D_{as} is a 2-qubit nonlocal unitary. Figure 1(a) can be rewritten as Fig. 1(b) by applying V'_a to the prepared ancilla state $|+\rangle_a$ and

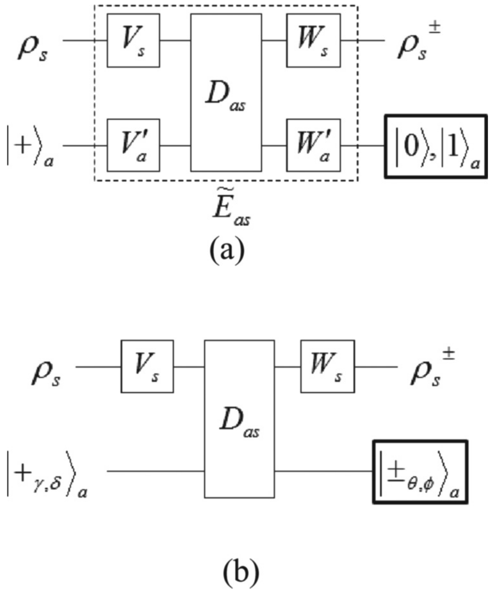

FIG. 1. ADQC. A rectangle box with bold line represents a measurement and the inside represents a basis for the measurement.

W'_a to the measurement basis $\{|0\rangle,|1\rangle\}$. D_{as} is described as

$$D_{as} = e^{-i(\alpha_x X_a \otimes X_s + \alpha_y Y_a \otimes Y_s + \alpha_z Z_a \otimes Z_s)}$$

by using nonsymmetric parameters $0 \leqslant \alpha_x, \alpha_y, \alpha_z \leqslant \frac{\pi}{4}$ due to the Weyl chamber [46].

For universal quantum computation, we should choose all the parameters appropriately. To this end, Anders *et al.* [15] derive sufficient conditions for (i) unitarity, (ii) *one-step* correctable branching, (iii) standardization, and (iv) universality. Especially, we will discuss one-step correctable branching, which states that the generalized Pauli correction according to the measurement outcome after "one" execution in ADQC enables the Kraus operator acting on the system deterministic. To fulfill these conditions, it is shown that the entangle operator $\tilde{E}_{as}$ must be locally equivalent to either SWAP + CZ ($\alpha_x = \alpha_y = \frac{\pi}{4}, \alpha_z = 0$) or CZ ($\alpha_x = \frac{\pi}{4}, \alpha_y = \alpha_z = 0$).

III. ANCILLA-DRIVEN UNIVERSAL BLIND QUANTUM COMPUTATION

ADQC of SWAP + CZ type can be considered as an extension of one-way quantum computation because the measurements are made on the system instead of on the ancilla if we exclude the SWAP and this case is exactly one-way quantum computation. So we can perform universal blind ADQC of the SWAP + CZ type as in [23]. In this paper, we focus only on universal blind ADQC of CZ type. Requiring all the conditions (i)–(iv) is too strong for universal blind ADQC of CZ type, since ADQC of CZ type satisfying all the conditions cannot be blind (in the sense of [23]) as is shown in the following. The system Kraus operator for $\tilde{E}_{as}$ is specified as $\tilde{K}_s^{\pm} = V_s K_s^{\pm} W_s$ and $K_s^{\pm} = {}_a\langle \pm_{\theta,\varphi}|D_{as}|+_{\gamma,\delta}\rangle_a$. As in [15], unitarity and one-step correctable branching require that the parameters for the ancilla satisfy $\sin\theta\cos\gamma\sin\phi = \cos\theta\sin\gamma\sin\delta$ and the Kraus operator $K_s^{\pm} = f_{\pm}I + i(-1)^{n_{\pm}}g_{\pm}X$, where $n_{\pm}$ are integers that differ in the parity. These coefficients are rewritten as

$$f_{\pm} = \frac{\cos\alpha_x}{\sqrt{2}}\sqrt{1 \pm \cos\gamma\cos\theta \pm \sin\gamma\sin\theta\cos(\delta - \phi)},$$
$$g_{\pm} = \frac{\sin\alpha_x}{\sqrt{2}}\sqrt{1 \mp \cos\gamma\cos\theta \pm \sin\gamma\sin\theta\cos(\delta + \phi)}.$$

Moreover, the parameter α_x for D_{as} and the parameters for the ancilla have the following relation:

$$\tan^2\alpha_x = \sqrt{\frac{1 - [\cos\gamma\cos\theta + \sin\gamma\sin\theta\cos(\delta - \phi)]^2}{1 - [\cos\gamma\cos\theta - \sin\gamma\sin\theta\cos(\delta + \phi)]^2}}.$$

Therefore, unitarity and one-step correctable branching imply that admissible parameters of the ancilla are classified into the following four cases.

Prepared ancilla	Measurement basis	Kraus operator
$\gamma = 0$	$\theta = 0$	$K_s^{\pm} = X^s I$
$\gamma = 0$	$\theta = \text{any}, \phi = 0$	$K_s^{\pm} = X^s R_x(\theta)$
$\gamma = \frac{\pi}{2}$	$\theta = 0$	$K_s^{\pm} = X^s X$
$\gamma, \delta = \text{any}$	$\theta = \frac{\pi}{2}, \phi = 0$	$K_s^{\pm} = X^s X$

For "universal" blind computation, a rotation operator $R_x(\theta)$ is indispensable. Thus, we consider only the second case. In that case, the prepared ancilla should be fixed to $|0\rangle$ since $\gamma = 0$. This means that we cannot use a random ancilla restricted on some plane in the Bloch sphere to make the computation blind similar to that in [23].

For that reason, we disregard one-step correctable branching for the present and derive some more admissible parameters of the ancilla as follows.

Prepared ancilla	Measurement basis	Kraus operator
$\gamma = \text{any}$, $\delta = 0$	$\theta = \text{any}$, $\phi = 0$	$K_s^{+} = \cos(\frac{\theta-\gamma}{2})I - i\sin(\frac{\theta+\gamma}{2})X$ $K_s^{-} = \sin(\frac{\theta-\gamma}{2})I + i\cos(\frac{\theta+\gamma}{2})X$
$\gamma, \delta = \text{any}$	$\theta = \gamma, \phi = \delta$	$K_s^{+} = I - i\sin\gamma\cos\delta X$ $K_s^{+} = (i\sin\delta - \cos\gamma\cos\delta)X$

Then, we have the Kraus operators written as

$$K_s^{+} = R_x(\gamma) \quad \text{and} \quad K_s^{-} = XR_x(-\gamma)$$

by choosing the prepared ancilla parameters γ to be any value and $\delta = 0$ and the measurement basis parameters $\phi, \theta = 0$. Blind ADQC of the CZ type is enabled by allowing the above Kraus operators. For blind computation, it is sufficient that all the information Client sends to Server is uniformly random. This is for hiding the rotation of unitaries to Server in the computation and we show a rough sketch to incorporate this idea into ADQC. First, Client chooses a prepared ancilla parameter γ randomly and Client sends ancilla $|+_{\gamma,0}\rangle$ or $|-_{\gamma,0}\rangle = |+_{\gamma+\pi,0}\rangle$ with equal probabilities. Then, Server performs the Kraus operator $R_x((-1)^s\gamma)$ using this ancilla. At this time, the ancilla is $\frac{1}{2}\sum_{r\in\{0,1\}}|+_{\gamma+r\pi,0}\rangle\langle+_{\gamma+r\pi,0}| = \frac{I}{2}$ as a maximally mixed state. Moreover, if we assume the input state $|\psi\rangle = \cos\frac{\theta'}{2}|+\rangle + e^{i\varphi'}\sin\frac{\theta'}{2}|-\rangle$, the output

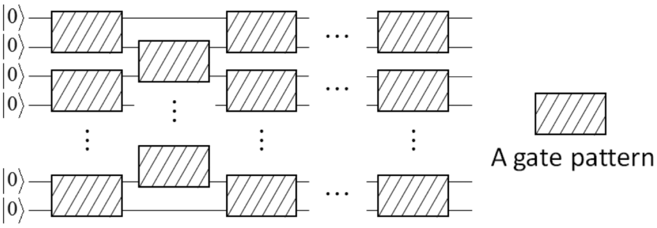

FIG. 2. Universal gate pattern.

state is $\frac{1}{2}\sum_{r\in\{0,1\}} R_x((-1)^s(\gamma+r\pi))|\psi\rangle\langle\psi|R_x^\dagger((-1)^s(\gamma+r\pi)) = (\begin{smallmatrix}\cos^2(\theta'/2) & 0\\ 0 & \sin^2(\theta'/2)\end{smallmatrix})$ so this state contains no information about γ. After that, Client sends a measurement basis parameter θ and Server performs the Kraus operator $R_x(\theta)$. Therefore, the total Kraus operator is $R_x(\theta+(-1)^s\gamma)$ and the total rotation of the Kraus operator is hiding to Server because γ is hiding. Based on this idea, we relax one-step correctable branching to *multiple step* and derive a sufficient condition which can make ADQC of the CZ type blind. *Multiple step* means that in "multiple" executions in ADQC, each Kraus operator need not be deterministic but the whole Kraus operator must be deterministic up to the correction.

For universal blind ADQC of CZ type, two types of Kraus operators are necessary. One type is an *uncorrectable* Kraus operator which depends on an outcome of the measurement, such as $V_s R_x((-1)^s\gamma)W_s$, performed using a prepared ancilla parameter γ. The other is a *correctable* Kraus operator, such as $V_s R_x(\theta)W_s$ up to Pauli correction, performed with a measurement basis parameter θ. With respect to these Kraus operators, we consider two conditions: *L-hiding* and *G-hiding*. L-hiding requires that $W_s R_x(\theta)V_s W_s R_x((-1)^s\gamma)V_s = W_s R_x(\theta')V_s W_s V_s \overset{\text{def}}{=} S$ holds, where $\theta' = \theta \pm (-1)^s\gamma$. G-hiding requires that a gate pattern which can perform both $U\otimes U'$ where U and U' are any 1-qubit unitaries and one kind of entangle operator is composable by using a unitary S and a controlled Pauli that can be simulated. In L-hiding, we might use an *assistant* Kraus operator, such as $W_s R_x(0)V_s$, for satisfying universality.

If the two conditions are satisfied, we can perform universal quantum computation by tiling the gate pattern in G-hiding regularly as in Fig. 2. What unitaries the gate pattern performs depends on a parameter θ' of each gate in L-hiding composing the gate pattern. When Client decides a parameter θ', Client sends a measurement basis parameter θ such that $\theta = \theta' \mp (-1)^s\gamma$. By choosing a prepared ancilla parameter γ randomly, θ also looks random to Server. This process is performed similarly to the protocol in [23]. We use the following protocol for the performance of each S.

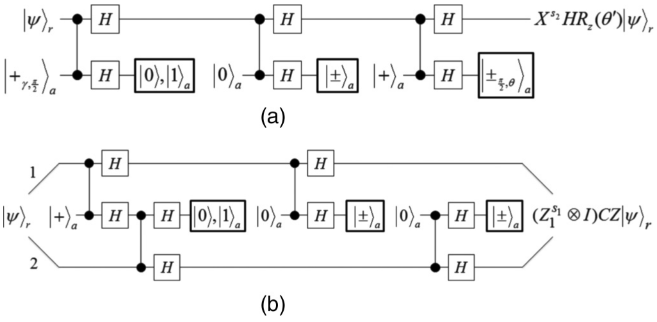
$|\psi\rangle_r$
$|+_{\gamma,\frac{\pi}{2}}\rangle_a$
H
$|0\rangle,|1\rangle_a$
$|0\rangle_a$
$|\pm\rangle_a$
$|+\rangle_a$
$|\pm_{\frac{\pi}{2},\theta}\rangle_a$
$X^{s_2}HR_z(\theta')|\psi\rangle_r$
(a)
1
2
$|\psi\rangle_r$
$|+\rangle_a$
$(Z_1^{s_1}\otimes I)CZ|\psi\rangle_r$
(b)

FIG. 3. Simulating (a) $H R_z(\theta')$ such that $\theta' = -\theta - (-1)^{s_1}\gamma$ and (b) CZ.

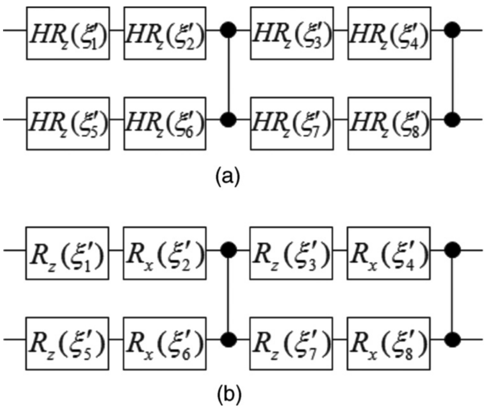

FIG. 4. Gate patterns for (a) a single entangle operator and (b) two entangle operators.

(1) Client chooses a prepared ancilla parameter γ randomly and sends the ancilla to Server.

(2) Server performs $W_s R_x((-1)^s\gamma)V_s$ with the given ancilla. Server sends an outcome s of the measurement in this simulation to Client.

(3) Client decides θ' and calculates $\theta = \theta' \mp (-1)^s\gamma + r\pi$ with a random bit $r \in \{0,1\}$ then sends θ to Server.

(4) Server performs $W_s R_x(\theta)V_s$ and sends an outcome s' of the measurement in this simulation to Client.

(5) Client inverts s' if $r = 1$.

If we use an assistant Kraus operator in the protocol, Server performs the corresponding simulation in step 2. In the above protocol, each ancilla state is maximally mixed and each θ looks random to Server. Therefore, the information leaked to Server is only the upper bound on the size of the universal gate pattern, that is, the upper bounds on the input size and the depth of the computation.

In the rest of this section, we discuss relations between the compatibility of the two hiding conditions and universality. When the protocol uses only one kind of entangle operator [e.g., $(H\otimes H)$CZ used in [14,15]] and no assistant Kraus operator, L-hiding and G-hiding do not hold simultaneously.

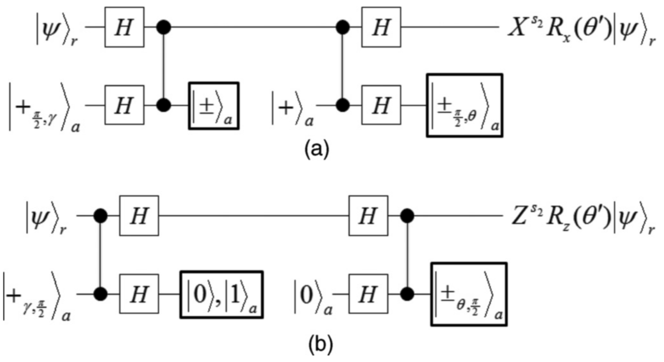
$|\psi\rangle_r$
$|+_{\frac{\pi}{2},\gamma}\rangle_a$
H
$|\pm\rangle_a$
$|+\rangle_a$
$|\pm_{\frac{\pi}{2},\theta}\rangle_a$
$X^{s_2}R_x(\theta')|\psi\rangle_r$
(a)
$|\psi\rangle_r$
$|+_{\gamma,\frac{\pi}{2}}\rangle_a$
$|0\rangle,|1\rangle_a$
$|0\rangle_a$
$|\pm_{\theta,\frac{\pi}{2}}\rangle_a$
$Z^{s_2}R_z(\theta')|\psi\rangle_r$
(b)

FIG. 5. Simulating $R_x(\theta')$ such that (a) $\theta' = -\theta + (-1)^{s_1}\gamma$ and (b) $\theta' = \theta - (-1)^{s_1}\gamma$.

From L-hiding, it must hold that $V_s W_s R_x((-1)^s\gamma) = R_x(\pm(-1)^s\gamma) V_s W_s$. By the similar discussion for universality in [15], $V_s W_s$ must be $aI + ibX$ or $aY + bZ$ up to a global phase, where $a,b \in \mathbb{R}$. Therefore, any 1-qubit unitary U composed of S is described as $U = W_s \tilde{U} V_s$ with the kernel $\tilde{U}$ which moves a quantum state only in some plane of the Bloch sphere, parallel to the Y-Z plane. If V_s and W_s are determined, U becomes a unitary which moves a quantum state only in one plane of the Bloch sphere so we cannot perform any arbitrary rotation $U \otimes U'$ in G-hiding. When the protocol uses an assistant Kraus operator, the two hiding conditions can hold simultaneously even if one kind of entangle operator [e.g., $(H \otimes H)$CZ] is allowed. It is enough to show how to simulate it and the gate pattern. The performance in L-hiding and a controlled-Pauli (CZ) in G-hiding are shown in Fig. 3. The gate pattern in G-hiding is shown in Fig. 4(a). When the protocol is allowed to use two kinds of entangle operators, the two hiding conditions can also hold simultaneously even if the protocol uses no assistant Kraus operator. To see that, the simulation in L-hiding is shown in Fig. 5 and the gate pattern in G-hiding is shown in Fig. 4(b). In summary, universal blind ADQC of CZ type is possible by considering *three-step* correctable branching when one kind of entangle operator is allowed in the protocol and *two-step* correctable branching when two kinds of entangle operators are allowed.

IV. CONCLUSION

In this Rapid Communication, we considered the possibilities and limitations for universal blind computation in ADQC. First, we proved that if we satisfy all the conditions for universal quantum computation in [15], we cannot perform universal blind computation. Therefore, we relaxed one condition and derived a sufficient condition for the blindness. Finally, we provided ways of universal blind computation in ADQC of CZ type.

Second, our way of universal blind ADQC needs fewer quantum requirements for Client than the approach taken in [23] in the case of using quantum inputs. In our way, Client does not need to rotate input states with respect to the Z axis in the Bloch sphere but only to apply Z. By extending our approach to a one-way model, we might also lower the quantum requirements in the one-way model.

[1] M. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, New York, 2000).

[2] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[3] D. Gross and J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007).

[4] G. K. Brennen and A. Miyake, Phys. Rev. Lett. **101**, 010502 (2008).

[5] A. Miyake, Phys. Rev. Lett. **105**, 040501 (2010).

[6] A. Miyake, Ann. Phys. (NY) **326**, 1656 (2011).

[7] T. C. Wei, I. Affleck, and R. Raussendorf, Phys. Rev. Lett. **106**, 070501 (2011).

[8] J. Cai, A. Miyake, W. Dur, and H. J. Briegel, Phys. Rev. A **82**, 052309 (2010).

[9] X. Chen, B. Zeng, Z. C. Gu, B. Yoshida, and I. L. Chuang, Phys. Rev. Lett. **102**, 220501 (2009).

[10] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007).

[11] Y. Li, D. E. Browne, L. C. Kwek, R. Raussendorf, and T. C. Wei, Phys. Rev. Lett. **107**, 060501 (2011).

[12] K. Fujii and T. Morimae, Phys. Rev. A **85**, 010304(R) (2012).

[13] T. Morimae, Phys. Rev. A **85**, 062328 (2012).

[14] J. Anders, D. K. L. Oi, E. Kashefi, D. E. Browne, and E. Andersson, Phys. Rev. A **82**, 020301(R) (2010).

[15] J. Anders, E. Andersson, D. E. Browne, E. Kashefi, and D. K. L. Oi, Theor. Comput. Sci. **430**, 51 (2012).

[16] R. Ionicioiu, T. P. Spiller, and W. J. Munro, Phys. Rev. A **80**, 012312 (2009).

[17] S. J. Devitt *et al.*, New J. Phys. **11**, 083032 (2009).

[18] T. P. Spiller *et al.*, New J. Phys. **8**, 30 (2006).

[19] P. van Loock, W. J. Munro, K. Nemoto, T. P. Spiller, T. D. Ladd, S. L. Braunstein, and G. J. Milburn, Phys. Rev. A **78**, 022303 (2008).

[20] A. M. Childs, Quant. Inf. Comput. **5**, 456 (2005).

[21] P. Arrighi and L. Salvail, Int. J. Quantum. Inform. **4**, 883 (2006).

[22] D. Aharonov, M. Ben-Or, and E. Eban, in *Proceedings of the 1st Symposium on Innovations in Computer Science (ICS 2010), Beijing* (Tsinghua University Press, Beijing, 2010).

[23] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual Symposium on Foundations of Computer Science (FOCS 2009), Atlanta* (IEEE, New York, 2009).

[24] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).

[25] T. Morimae, V. Dunjko, and E. Kashefi, arXiv:1009.3486.

[26] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).

[27] T. Morimae and K. Fujii, Nat. Commun. **3**, 1036 (2012).

[28] T. Morimae and K. Fujii, Phys. Rev. A **87**, 050301(R) (2013).

[29] J. F. Fitzsimons and E. Kashefi, arXiv:1203.5217.

[30] M. A. Nielsen and C. M. Dawson, Phys. Rev. A **71**, 042323 (2005).

[31] P. Aliferis and D. W. Leung, Phys. Rev. A **73**, 032308 (2006).

[32] M. Varnava, D. E. Browne, and T. Rudolph, Phys. Rev. Lett. **97**, 120501 (2006).

[33] T. Morimae and K. Fujii, Sci. Rep. **2**, 508 (2012).

[34] S. D. Barrett and T. M. Stace, Phys. Rev. Lett. **105**, 200502 (2010).

[35] K. Fujii and Y. Tokunaga, Phys. Rev. Lett. **105**, 250503 (2010).

[36] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, Phys. Rev. Lett. **105**, 250502 (2010).

[37] M. Van den Nest, A. Miyake, W. Dur, and H. J. Briegel, Phys. Rev. Lett. **97**, 150504 (2006).

[38] T. Morimae, Phys. Rev. A **81**, 060307(R) (2010).

[39] D. Gross, S. T. Flammia, and J. Eisert, Phys. Rev. Lett. **102**, 190501 (2009).

[40] M. J. Bremner, C. Mora, and A. Winter, Phys. Rev. Lett. **102**, 190502 (2009).

[41] F. Verstraete and J. I. Cirac, Phys. Rev. A **70**, 060302(R) (2004).

[42] M. Van den Nest, W. Dur, and H. J. Briegel, Phys. Rev. Lett. **98**, 117207 (2007).

[43] M. Van den Nest, W. Dur, and H. J. Briegel, Phys. Rev. Lett. **100**, 110501 (2008).

[44] K. Fujii and T. Morimae, Phys. Rev. A **85**, 032338 (2012).

[45] N. Khaneja, R. Brockett, and S. J. Glaser, Phys. Rev. A **63**, 032308 (2001).

[46] R. R. Tucci, arXiv:quant-ph/0507171.