Continuous-Variable Blind Quantum Computation

Tomoyuki Morimae*

Department of Physics, Imperial College London, London SW7 2BW, United Kingdom

(Received 30 August 2012; published 5 December 2012)

Blind quantum computation is a secure delegated quantum computing protocol where Alice, who does not have sufficient quantum technology at her disposal, delegates her computation to Bob, who has a fully fledged quantum computer, in such a way that Bob cannot learn anything about Alice's input, output, and algorithm. Protocols of blind quantum computation have been proposed for several qudit measurement-based computation models, such as the graph state model, the Affleck-Kennedy-Lieb-Tasaki model, and the Raussendorf-Harrington-Goyal topological model. Here, we consider blind quantum computation for the continuous-variable measurement-based model. We show that blind quantum computation is possible for the infinite squeezing case. We also show that the finite squeezing causes no additional problem in the blind setup apart from the one inherent to the continuous-variable measurement-based quantum computation.

DOI: 10.1103/PhysRevLett.109.230502 PACS numbers: 03.67.Lx, 03.67.Dd

Introduction.—When a scalable quantum computer is realized, it will be used in the ''cloud'' style since only a limited number of people will be able to possess quantum computers. Blind quantum computation [1–11] provides a solution to the issue of the client's security in such a cloud quantum computation. Blind quantum computation is a new secure protocol which enables Alice, who does not have enough quantum technology, to delegate her computation to Bob, who has a fully fledged quantum computer, in such a way that Bob cannot learn anything about Alice's input, output, and algorithm. A protocol of the unconditionally secure universal blind quantum computation was first proposed in Ref. [3] by using the measurement-based quantum computation (MBQC) on the cluster state [12–14] and later generalized to other resource states such as the Affleck-Kennedy-Lieb-Tasaki state [5,15,16] and the three-dimensional Raussendorf-Harrington-Goyal state [17–21], which enables topological fault tolerance [8,9]. A proof-of-principle experiment of blind computation was realized by using the discrete degrees of freedom of photons [7].

In this paper, we consider the continuous variable (CV) version of the blind quantum computation. The CV cluster MBQC was proposed in Refs. [22,23]. There, $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ state of a single qubit is replaced with the zero momentum state $|0\rangle_p$ of a single mode (qumode), and the two-mode gate $e^{iq\otimes q}$ plays the role of the qubit CONTROLLED-Z gate, $|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes Z$. Experimental demonstrations of the building blocks of the CV cluster MBQC were already achieved [24–28]. We show that blind quantum computation is possible in the infinite squeezing case. We also consider the finite squeezing case and show that it causes no problem apart from the additional errors, which come from the redundancy of gates required for the blindness. Since even the nonblind CV MBQC has to cope with these errors for its scalability, we conclude that the finite squeezing does not cause any fundamental problem in principle.

CV cluster MBQC.—Let us briefly review the CV cluster MBQC proposed in Refs. [22,23]. We define the Weyl-Heisenberg operators $X(s) \equiv \exp[-isp]$ and $Z(s) \equiv \exp[isq]$ with $s \in \mathbb{R}$, where q and p are the quadrature operators. These Weyl-Heisenberg operators are CV analog of the qubit Pauli operators. The Fourier transform operator F is defined by $F \equiv \exp[i(q^2+p^2)\frac{\pi}{4}]$ with $F|s\rangle_q = |s\rangle_p$. This operator is the CV analog of the qubit Hadamard operator. The CV version of the CONTROLLED-Z gate and the CONTROLLED-X gate are defined by $CZ \equiv \exp(iq\otimes q)$ and $CX \equiv \exp(-iq\otimes p)$, respectively. The elementary block of the CV cluster MBQC is the teleportation gate (Fig. 1). Here, $D_q^f \equiv \exp[if(q)]$, and f is a polynomial of q. Note that D_q^f and D_p^f are obtained from FD_q^f since $(FD_q^0)^3 FD_q^f = D_q^f$ and $(FD_q^0)^2(FD_{-q}^f)(FD_q^0) = D_p^f$. Furthermore, $e^{isq^k/k}$ $(k = 1, 2, 3)$ and $e^{isp^k/k}$ $(k = 1, 2, 3)$ are single-mode universal [29]. Hence, $R_q(v) \equiv F\exp[i(aq + b\frac{q^2}{2} + c\frac{q^3}{3})]$ is single-mode universal, where $v = (a, b, c)$. The addition of CZ enables all multimode universality. Let us explain how to compensate the by-product error $X(m)$ in Fig. 1. Note that $R_q(v)X(m) = Z(m)R_{q+m}(v) = Z(m)R_q(M_m v)$, where

$$M_m = \begin{pmatrix} 1 & m & m^2 \\ 0 & 1 & 2m \\ 0 & 0 & 1 \end{pmatrix}.$$

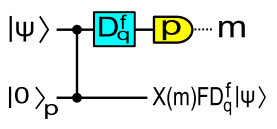

FIG. 1 (color online). The CV teleportation gate.

 © 2012 American Physical Society

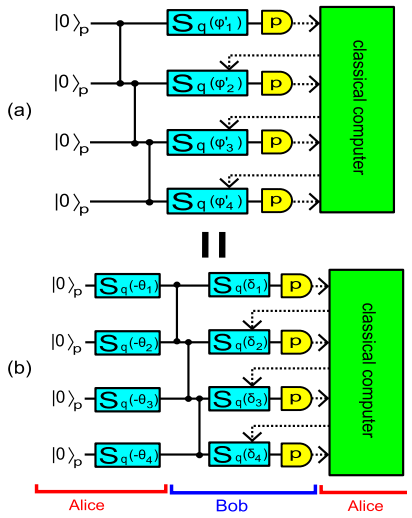

FIG. 2 (color online). (a): The circuit representation of the CV MBQC, where $S_q(\phi) = F^\dagger R_q(\phi)$. (b): The blind version of (a). Since S_q's commute with CZ's (b) is equivalent to (a).

Therefore, if we want to implement $R_q(v)$ and if there is the by-product $X(m)$, we have only to implement $R_q(M_m^{-1}v)$. In short, Fig. 2(a) is universal if the feed forwarding is appropriately done. Finally, let us notice that the zero-momentum state $|0\rangle_p$ is not realistic, and normally $|0\rangle_p$ is approximated by the finitely squeezed vacuum state $|0,\Omega\rangle_p = (\pi\Omega^2)^{-1/4}\int dp e^{-(p^2/2\Omega^2)}|p\rangle_p$. This finite squeezing causes errors in the CV cluster MBQC [22,23].

Blind quantum computation.—In the blind quantum computation [3], Alice, the client, has a quantum device which emits randomly rotated single qubit states and a classical computer. Bob, the server, has full quantum power. Let us assume that Alice wants to perform the cluster MBQC on the N-qubit graph state $|G\rangle$ with measurement angles $\{\phi_j\}_{j=1}^N$. If Alice sends Bob $\{\phi_j\}_{j=1}^N$, and Bob creates $|G\rangle$, the delegated quantum computation is of course possible. However, obviously in this case Bob can learn Alice's computation. Hence, they run the following protocol [3]: (1) Alice sends Bob N randomly rotated single-qubit states $\{|+_{\theta_j}\rangle\}_{j=1}^N$, where $|+_\theta\rangle \equiv e^{-iZ\theta/2}|+\rangle$ and $\theta_j \in \{\frac{k\pi}{4}|k = 0, 1, \ldots, 7\}$ is a random angle, which is hidden from Bob. (2) Bob applies CZ gates among them according to the graph structure. Since CZ commutes with $e^{-iZ\theta/2}$, Bob obtains $(\bigotimes_{e\in E} CZ_e)\times(\bigotimes_{j=1}^N e^{-iZ_j\theta_j/2})|+\rangle^{\otimes N} = (\bigotimes_{j=1}^N e^{-iZ_j\theta_j/2})|G\rangle$, where E is the set of edges of G, and the subscript j of Z_j means the operator acts on jth qubit. (3) For $j = 1$ to N, they repeat the following: Alice sends Bob $\delta_j \equiv \theta_j + \phi'_j + r_j\pi$, where ϕ'_j is the modification of ϕ_j which includes appropriate feed forwardings (by-product corrections) and $r_j \in \{0, 1\}$ is a random binary, which is hidden from Bob. Next, Bob measures jth qubit in the $\{|\pm_{\delta_j}\rangle\}$ basis and returns the measurement result to Alice.

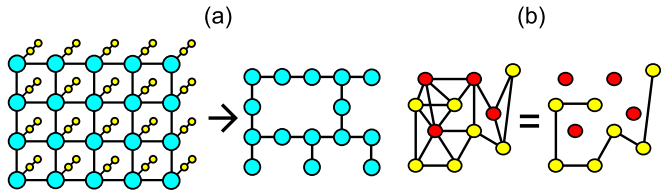

FIG. 3 (color online). (a) The hair implantation technique [8]. Left: A two-qubit graph state (hair) indicated by yellow (small circle) is attached to each blue qubit (large circle) of the square graph state. Right: A desired graph state can be carved out from the blue square graph. Bob cannot know this graph structure. (b) The graph hiding technique [9]. Yellow qubits (some qubits) are $|+_\theta\rangle$, whereas red qubits (other qubits) are $|0\rangle$ or $|1\rangle$. Bob applies CZ gates on all edges (the left) but actually obtains the right graph state, and he does not know its geometry.

It was shown in Ref. [3] that this protocol is correct. Here, correct means that if Bob is honest then Alice obtains the correct outcome. It was also shown that the protocol is blind [3]. Here, blind means that whatever Bob does, Bob cannot learn anything about Alice's input, output, and algorithm.

In order to guarantee Alice's privacy, the geometry of graph G must be a secret to Bob. There are three ways of doing it. The first technique is to use the brickwork state [3]: a certain two-dimensional graph state, which is universal with only $\{|\pm_\theta\rangle\}$ basis measurements for $\theta \in \{\frac{k\pi}{4}|k = 0, 1, \ldots, 7\}$. Since the geometry of the brickwork state is fixed, Bob cannot learn about Alice's algorithm. The second technique is to implant a "hair" to each qubit of the regular-lattice graph state [8] as shown in Fig. 3(a). We can simulate Z measurement and any X-Y plane measurement on any blue qubit with only X-Y plane measurements on yellow and blue qubits [8]. Hence, we can "carve out" a specific graph structure from the square lattice of blue qubits, as shown on the right side of Fig. 3(a). The third technique is the "graph hiding technique" [9]. By using this technique, Alice can have Bob prepare any graph state in such a way that Bob cannot learn the geometry of the graph. This technique is based on the simple idea that CZ does not create entanglement if one of the qubits is $|0\rangle$ or $|1\rangle$: $CZ(|\psi\rangle\otimes|0\rangle) = |\psi\rangle\otimes|0\rangle$ and $CZ(|\psi\rangle\otimes|1\rangle) = Z|\psi\rangle\otimes|1\rangle$. Therefore, if Alice hides several qubits in $|0\rangle$ or $|1\rangle$ into the set of qubits she initially sends to Bob, she can let Bob create her desired graph state. Since Bob cannot distinguish $|0\rangle$, $|1\rangle$, and eight $|+_\theta\rangle$ states, Bob cannot know when he entangles qubits [Fig. 3(b)].

CV blind protocol.—Now let us explain our CV blind protocol. Our protocol runs as follows: (1) Alice sends Bob N qumode states $\{S_q(-\theta_j)|0\rangle_p\}_{j=1}^N$, where $\theta_j = (a_j, b_j, c_j)$ is randomly chosen from $\mathbb{R}^3$ and $S_q(v) = F^\dagger R_q(v)$. (2) Bob applies CV CZ gates according to the graph structure. (3) Alice might choose the brickwork, the hair implantation technique, or the graph hiding technique. Regardless of her choice, we can assume without loss of generality that Bob has the "encrypted" CV graph state $[\bigotimes_{j=1}^N X^j(\xi_j)Z^j(\eta_j)S_q^j(-\theta_j)]|G\rangle$, where $|G\rangle$ is the

N-qumode CV graph state, and the subscript j of X^j means it acts on the jth qumode. (3) For $j = 1$ to N, Alice and Bob repeat the following: let $\phi_j \equiv (\alpha_j, \beta_j, \gamma_j)$ be Alice's computational parameters (her algorithm), and let $\phi'_j \equiv (\alpha'_j, \beta'_j, \gamma'_j)$ include feed forwardings. Alice sends Bob $\delta_j = M_{\xi_j}^{-1} w_j$, where $w_j = (\alpha'_j + a_j - \eta_j + r_j, \beta'_j + b_j, \gamma'_j + c_j)$ and $r_j \in \mathbb{R}$ is a random real number. Next, Bob applies $S_q(\delta_j)$ on jth qumode and does the p measurement. (Or, he directly measures $S_q^\dagger(\delta_j) p S_q(\delta_j)$ of the jth qumode.) He sends the measurement result to Alice.

Correctness.—Let us show the correctness of our protocol. See Fig. 2(b), which is the circuit representation of our protocol. Since S_q commutes with CZ, Fig. 2(b) is equivalent to Fig. 2(a). Note that the equivalence between (a) and (b) in Fig. 2 is based on only the commutativity between S_q and CZ; therefore, it holds even if we replace each input $|0\rangle_p$ with its finitely squeezed version. Hence, the finite squeezing does not cause any additional effect here.

More precisely, note that the following is true for any state $|\psi\rangle$:

$$
\begin{aligned}
{}_p\langle p|S_q^j(\delta_j)X^j(\xi_j)Z^j(\eta_j)S_q^j(-\theta_j)|\psi\rangle &= {}_p\langle p|X^j(\xi_j)Z^j(\eta_j)S_q^j(M_{\xi_j}M_{\xi_j}^{-1}w_j)S_q^j(-\theta_j)|\psi\rangle \\
&= {}_p\langle p|X^j(\xi_j)Z^j(\eta_j)S_q^j(w_j)S_q^j(-\theta_j)|\psi\rangle \\
&= {}_p\langle p|\exp\Big[i\Big\{(\alpha'_j + a_j - \eta_j + r_j)q + (\beta'_j + b_j)\frac{q^2}{2} + (\gamma'_j + c_j)\frac{q^3}{3} \\
&\quad + \eta_j q - a_j q - b_j\frac{q^2}{2} - c_j\frac{q^3}{3}\Big\}\Big]|\psi\rangle \\
&= {}_p\langle p|\exp[ir_j q]\exp\Big[i\Big\{\alpha'_j q + \beta'_j\frac{q^2}{2} + \gamma'_j\frac{q^3}{3}\Big\}\Big]|\psi\rangle \\
&= {}_p\langle p|\exp[ir_j q]S_q^j(\phi'_j)|\psi\rangle \\
&= {}_p\langle p - r_j|S_q^j(\phi'_j)|\psi\rangle.
\end{aligned}
$$

Hence, Bob effectively does the correct MBQC except for the fact that if the measurement result is p, the by-product, which comes from this measurement, is not $X(p)$ but $X(p - r_j)$; the by-product can be compensated by changing the following measurement parameter: since the above equation is true for any state $|\psi\rangle$, the situation does not change even if the squeezing is finite.

The brickwork implementation for the CV blind protocol is shown in Fig. 4. Since $CZ \times CZ \neq I$ for the CV case, we cannot directly generalize the qubit brickwork state of Ref. [3] to the CV case. In particular, we need CZ and $CZ^\dagger$ as is shown in the figure. The hair implantation technique also works if we implant four-qumode hair on each qumode, since the measurement of q on a qumode in a CV graph state removes that qumode [23], and a q measurement can be simulated only with $S_q^\dagger p S_q$ measurements by using the following relations: $F \times Fe^{iq^2/2} \times Fe^{iq^2/2} \times F = e^{iq^2/2}e^{ip^2/2}$ and $e^{-ip^2/2}e^{-iq^2/2}pe^{iq^2/2}e^{ip^2/2} = q$. The graph hiding technique for qubits can also be generalized to CV, since

$$
\begin{aligned}
CZ(|\psi\rangle \otimes |s\rangle_p) &= (I \otimes Z(s))CZ(|\psi\rangle \otimes |0\rangle_p), \\
CZ(|\psi\rangle \otimes |s\rangle_q) &= (Z(s)|\psi\rangle) \otimes |s\rangle_q.
\end{aligned}
\tag{1}
$$

Therefore, Alice can have Bob create a graph state in such a way that Bob cannot know the graph geometry.

Finally, let us consider the effect of the finite squeezing. As we have seen, the equivalence between Figs. 2(a) and 2(b) is valid for any initial state (Fig. 2); therefore, the finite squeezing does not cause any additional problem apart from the original one inherent to the nonblind CV MBQC [22,23]. If Alice and Bob choose the brickwork implementation or the hair implantation technique, the finite squeezing does not cause any additional effect since the brickwork blind quantum computation and the hair implantation technique are nothing but a normal cluster MBQC with some redundant gates. (Of course, this redundancy accelerates the accumulation of errors, and, therefore, requires more fault tolerance, but such a problem is not a specific problem to the blind CV MBQC. Even the nonblind one ultimately needs

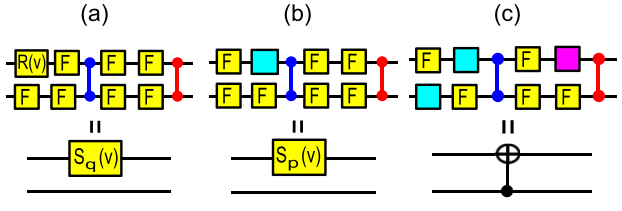

FIG. 4 (color online). (a) The implementation of $S_q(v) \otimes I$. Blue (left) two-qubit gate is CZ. Red (right) two-qubit gate is $CZ^\dagger$. (b) The implementation of $S_p(v) \otimes I$. The blue (empty) box means $R_{-q}(M_m^{-1}v)$. (c) The implementation of CX. The blue boxes are $Fe^{iq^2/2}$ up to by-product corrections. The purple (right empty) box is $Fe^{-iq^2/2}$ up to by-product corrections.

enough fault tolerance for the scalability [22,23,26,30].) Finally, regarding the graph hiding technique, once the graph state is created, it is a usual CV MBQC with errors. If the squeezing is finite, Eq. (1) becomes not an exact but approximate one. This causes additional errors on the created graph state, but such errors are that even the nonblind CV MBQC can experience.

Blindness.—In our protocol, Bob obtains quantum states $\{S_q(-\theta_j)|0\rangle_p\}_{j=1}^N$ and classical messages $\{\delta_j\}_{j=1}^N$. Note that $\theta_j = M_{\xi_j}\delta_j - \phi_j' + \eta_j e - r_j e \equiv k_j - r_j e$, where $e = (1, 0, 0)$. Hence, Bob's state is

$$\int dr \bigotimes_{j=1}^N S_q(-\theta_j)|0\rangle_{pp}\langle 0|S_q^\dagger(-\theta_j) = \int dr \bigotimes_{j=1}^N S_q(-k_j)|r_j\rangle_{pp}\langle r_j|S_q^\dagger(-k_j) = I^{\otimes N},$$

which means that Bob's state is independent of $\{\phi_j\}_{j=1}^N$. Note that the blindness also holds in the finite squeezed case, since

$$\int dr \bigotimes_{j=1}^N S_q(-\theta_j)|0, \Omega_j\rangle_{pp}\langle 0, \Omega_j|S_q^\dagger(-\theta_j) = \int dr \bigotimes_{j=1}^N T_{\Omega_j}[S_q(-k_j)e^{ir_j q}|0\rangle_{pp} \times \langle 0|e^{-ir_j q}S_q^\dagger(-k_j)]T_{\Omega_j}^\dagger,$$

where $T_\Omega \equiv (\pi\Omega^2)^{-1/4}\int dt e^{-(t^2/2\Omega^2)}e^{iqt}$.

Discussion.—In optical systems, the implementation of $e^{iq^3/3}$ is much harder than those of e^{iq} and $e^{iq^2/2}$. Hence it would be desirable for Alice to avoid the implementation of $e^{iq^3/3}$ by herself. There are two solutions. One solution is for Bob to embed many $e^{isq^3/3}|0\rangle_p$ with various s into his resource state. If Alice uses the hair implantation technique or the graph hiding technique, Bob cannot know which $e^{isq^3/3}|0\rangle_p$ contributes to the computation. The other solution is to use the relation

$$Q^\dagger(t)e^{i\gamma q^3/3}Q(t) = e^{i\gamma' q^3/3}, \quad (2)$$

where $Q(t) \equiv e^{-i\ln(t)(qp+pq)/2}$ is the squeezing and $t = (\gamma'/\gamma)^{1/3}$. Since the squeezing can be done blindly, Alice can have Bob implement $e^{i\gamma' q^3/3}$ without allowing Bob to learn γ'.

If the state measurement is relatively easy, we can consider another blind quantum computation protocol, where Bob creates the resource state and Alice does the measurement [10]. One advantage of this protocol is that the security is guaranteed by the no-signaling principle [31], which is more fundamental than quantum physics, and Alice does not need to verify her measurement device (the device independence [32]). The CV cluster MBQC is suitable for such a measuring Alice protocol,

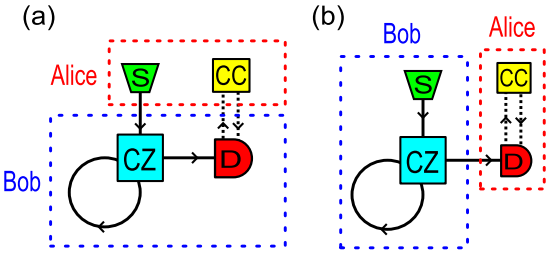

FIG. 5 (color online). Blind version of the temporal encoding [33]. S is the squeezed state source, D is the measurement device, CZ is the machine which implements the CZ gate, and CC is a classical computer.

since the measurements of $e^{-isq}pe^{isq} = p + s$ and $e^{-isq^2/2}pe^{isq^2/2} = p + sq$ are easily done with the homodyne detection. The gate $e^{isq^3/3}$ can be implemented blindly by using Eq. (2).

If we use the temporal degrees of freedom, only a single CZ machine is sufficient [33]. As shown in Fig. 5, it is easy to see that blind versions of such a temporal encoding implementation are possible whether Alice prepares states [Fig. 5(a)] or does the measurements [Fig. 5(b)].

The author acknowledges JSPS for support.

*morimae@gmail.com

[1] A. Childs, Quantum Inf. Compt. **5**, 456 (2005).
[2] P. Arrighi and L. Salvail, Int. J. Quantum. Inform. **04**, 883 (2006).
[3] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, USA, 2009), p. 517.
[4] D. Aharonov, M. Ben-Or, and E. Eban, *Proceeding of Innovation in Computer Science* (Tsinghua University Press, Beijing, China, 2010), p. 453.
[5] T. Morimae, V. Dunjko, and E. Kashefi, arXiv:1009.3486.
[6] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).
[7] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
[8] T. Morimae and K. Fujii, Nat. Commun. **3**, 1036 (2012).
[9] J. F. Fitzsimons and E. Kashefi, arXiv:1203.5217.
[10] T. Morimae and K. Fujii, arXiv:1201.3966.
[11] T. Morimae, arXiv:1208.1495.
[12] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[13] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[14] R. Raussendorf, Ph.D. thesis, Ludwig-Maximillians Universität München, 2003.
[15] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki, Commun. Math. Phys. **115**, 477 (1988).
[16] G. K. Brennen and A. Miyake, Phys. Rev. Lett. **101**, 010502 (2008).
[17] R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).

[18] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007).
[19] R. Raussendorf, J. Harrington, and K. Goyal, Ann. Phys. (Amsterdam) **321**, 2242 (2006).
[20] Y. Li, D. E. Browne, L. C. Kwek, R. Raussendorf, and T. C. Wei, Phys. Rev. Lett. **107**, 060501 (2011).
[21] K. Fujii and T. Morimae, Phys. Rev. A **85**, 010304(R) (2012).
[22] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Phys. Rev. Lett. **97**, 110501 (2006).
[23] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, Phys. Rev. A **79**, 062318 (2009).
[24] R. Ukai, S. Yokoyama, J. Yoshikawa, P. van Loock, and A. Furusawa, Phys. Rev. Lett. **107**, 250501 (2011).
[25] Y. Miwa, R. Ukai, J. Yoshikawa, R. Filip, P. van Loock, and A. Furusawa, Phys. Rev. A **82**, 032305 (2010).
[26] R. Ukai, N. Iwata, Y. Shimokawa, S. C. Armstrong, A. Politi, J. Yoshikawa, P. van Loock, and A. Furusawa, Phys. Rev. Lett. **106**, 240504 (2011).
[27] M. Yukawa, R. Ukai, P. van Loock, and A. Furusawa, Phys. Rev. A **78**, 012301 (2008).
[28] Y. Miwa, J. Yoshikawa, P. van Loock, and A. Furusawa, Phys. Rev. A **80**, 050303(R) (2009).
[29] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
[30] M. Ohliger, K. Kieling, and J. Eisert, Phys. Rev. A **82**, 042336 (2010).
[31] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[32] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[33] N. C. Menicucci, X. Ma, and T. C. Ralph, Phys. Rev. Lett. **104**, 250503 (2010).