Long-Distance Measurement-Device-Independent Multiparty Quantum Communication

Yao Fu, Hua-Lei Yin, Teng-Yun Chen, and Zeng-Bing Chen*
Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China and The CAS Center for Excellence in QIQP and the Synergetic Innovation Center for QIQP, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China
(Received 28 September 2014; published 2 March 2015)

The Greenberger-Horne-Zeilinger (GHZ) entanglement, originally introduced to uncover the extreme violation of local realism against quantum mechanics, is an important resource for multiparty quantum communication tasks. But the low intensity and fragility of the GHZ entanglement source in current conditions have made the practical applications of these multiparty tasks an experimental challenge. Here we propose a feasible scheme for practically distributing the postselected GHZ entanglement over a distance of more than 100 km for experimentally accessible parameter regimes. Combining the decoy-state and measurement-device-independent protocols for quantum key distribution, we anticipate that our proposal suggests an important avenue for practical multiparty quantum communication.

DOI: 10.1103/PhysRevLett.114.090501 PACS numbers: 03.67.Dd, 03.65.Ud, 03.67.Ac, 03.67.Hk

Remote distribution of quantum signals (photonic states) is an essential task in the realm of quantum communication. Quantum key distribution (QKD) allows the information-theoretically secure transmission of classical messages and requires delivery of either single photons in the case of BB84 protocol [1], or entangled photons in the case of Ekert91 protocol [2]. Remote distribution of entanglement also enables certain classically impossible tasks, such as quantum teleportation of unknown states and quantum dense coding [3]. Up to now, tremendous effort has been dedicated to increasing the transmission distance of quantum communication between *two* legitimate users. The recorded distance for QKD has been more than 300 km for standard telecom fiber links [4], while quantum teleportation has been demonstrated over a distance of more than 100 km for free-space channels [5].

So far, most theoretical and experimental works on quantum communication are focused on two-party protocols. Yet, multiparty quantum communication protocols do exist, as illustrated by the fascinating examples such as quantum cryptographic conferencing (QCC) [6,7], quantum secret sharing (QSS) [8–11] and third-man quantum cryptography [12]. These multiparty protocols require an important resource—the Greenberger-Horne-Zeilinger (GHZ) entangled states [13,14] with perfect multiparty quantum correlations, which are originally introduced to reveal the extreme violation of local realism against quantum mechanics. Nevertheless, the practical applications of GHZ states are quite limited due to the lack of two important factors—the high-intensity source and remote reliable distribution of the GHZ states. The existing experimental works [10] on multiparty quantum communication remain the proof-of-principle demonstration and reported rather low key rates. The experimental distribution of the GHZ entanglement [15] was achieved only recently, over a distance of less than 1 km for each party of the GHZ-entangled photons. Thus, the current status of multiparty quantum communication still remains an extreme experimental challenge even under the state-of-the-art technologies and is far from practical applications. In this Letter, we propose a feasible scheme for distributing the postselected GHZ entanglement over a distance of more than 100 km for experimentally relevant parameter regimes. Combining the decoy-state QKD [16] and the measurement-device-independent (MDI) QKD [17] technologies, our findings manifest the possibility for practical applications of MDI multiparty quantum communication such as QCC and QSS, as well as for the long-distance GHZ experiment.

Multiparty quantum communication protocols aim to provide information-theoretic security for highly sensitive and confidential multiuser communication based on the laws of quantum mechanics, which physically outperform their classical counterparts. Their applications [8,9,11] range from the secret multiparty conference, remote voting, online auctioning, master key of the payment system, jointly checking accounts containing quantum money [18], to secure distributed quantum computation [19]. Among them, QCC is a protocol for multiparty QKD [6], which requires a common random bit sequence (the keys) to be securely shared among the legitimate users even in the presence of any eavesdropper. QSS is a protocol of splitting a message into several parts among a group of participants, each of whom is allocated a share of the secret [8]. As a consequence, only the entire set is sufficient to read the message thoroughly. For example, QSS can be used to guarantee that no single person can launch a nuclear missile, or open a bank vault, but all legitimate users together can.

Before we describe our multiparty communication schemes in detail, let us recapitulate the significance of the GHZ state $|\Phi_0^{\pm}\rangle = 1/\sqrt{2}(|HHH\rangle \pm |VVV\rangle)$, where $|H\rangle$ and $|V\rangle$ represent photonic horizontal and vertical polarizations, respectively. If three members of a GHZ state are measured along Z basis, each of them will give a random outcome, Z_A, Z_B, Z_C, and the outcomes of the three members will always be in perfect correlations, $Z_A = Z_B = Z_C$, which can be used for multiparty quantum cryptographic conferencing. Likewise, when three members of a GHZ state $|\Phi_0^{+}\rangle$ ($|\Phi_0^{-}\rangle$) are measured along X basis, each will give a random outcome, i.e., X_A, X_B, X_C, whose sharing of a binary correlation $X_A = X_B \oplus X_C$ ($X_A \oplus 1 = X_B \oplus X_C$) will always hold and can then be used for multiparty QSS. Besides, when Alice announces her measurement result X_A, Bob and Charlie will have a perfect correlation which can be used for third-man quantum cryptography.

Here we exploit an approach that requires neither the preparation in advance nor the distribution of high-fidelity GHZ entangled states through a long distance. The design is to take advantage of postselected GHZ states among three legitimate users (typically called Alice, Bob, and Charlie) to perform information-theoretically secure multiparty quantum communication. Like the MDI-QKD protocol [17], the postselecting measurement device here can be regarded as a black box which can be manipulated by anyone, even the eavesdropper. Therefore, our scheme is naturally immune to all detection-side attacks and can be regarded as the combination of time-reversed GHZ state distribution and measurement. Together with the decoy-state method [16], in which pulses with different amplitudes are randomly mixed and phases are randomized, our scheme is able to defeat photon-number-splitting attacks [20]. We utilize conventional laser sources to obtain a long distribution distance between the middle node and users for both the MDI-QCC and MDI-QSS protocols. Similarly to the security proof of QKD [17,21], we use the multiparty entanglement purification technique [22] to provide information-theoretically secure information transmission. The security of our protocols is analyzed in the Supplemental Material [23].

In the following, let us explain our MDI-QCC and MDI-QSS protocols in more detail. The main quantum procedures of the two schemes are the same, while the difference lies in their classical postprocessing. The MDI-QCC (MDI-QSS) protocol uses the data in Z (X) basis to extract secure keys. Our setup is depicted in Fig. 1. Here, we take MDI-QCC protocol as an example. Alice, Bob, and Charlie independently and randomly prepare quantum states with phase-randomized weak coherent pulses in two complementary bases (Z basis and X basis). They send the pulses to the untrusted fourth party located in the middle node, David, to perform a GHZ-state measurement which projects the incoming signals onto a GHZ state. Such a measurement can be realized, for instance, using only linear optical elements [33]. Actually, this procedure only identifies two of the eight GHZ states, while the identification of any one GHZ state is enough to prove the security. A successful GHZ-state measurement corresponds to the observation of three out of six detectors being clicked simultaneously. The clicks in $D1H$, $D2H$, and $D3H$, or in $D1H$, $D2V$, and $D3V$, or in $D1V$, $D2H$, and $D3V$, or in $D1V$, $D2V$, and $D3H$, imply a projection onto the GHZ state $|\Phi_0^{+}\rangle = 1/\sqrt{2}(|HHH\rangle + |VVV\rangle)$, while the clicks in $D1H$, $D2H$, and $D3V$, or in $D1H$, $D2V$, and $D3H$, or in $D1V$, $D2H$, and $D3H$, or in $D1V$, $D2V$, and $D3V$, indicate a projection onto the GHZ state $|\Phi_0^{-}\rangle = 1/\sqrt{2}(|HHH\rangle - |VVV\rangle)$. David announces the events through public channels whether he has obtained a GHZ state and which GHZ state he has received. Alice, Bob, and Charlie only keep the raw data of successful GHZ-state measurements and discard the rest. They postselect the events where they use the same basis in their transmission through an authenticated public channel. Notice that Alice performs a bit flip when Alice, Bob, and Charlie all choose X basis and David obtains a GHZ state $|\Phi_0^{-}\rangle$. We employ the data of Z basis to generate the cryptographic conferencing keys, while the data of X basis are totally used to estimate errors. Alice, Bob, and Charlie estimate the gain and quantum bit error rate with the decoy-state method, given that all of them send out single-photon states. Afterwards, they extract secure cryptographic conferencing keys after classical error correction and privacy amplification.

In the asymptotic limit, the MDI-QCC key generation rate is given by [17,22,34]

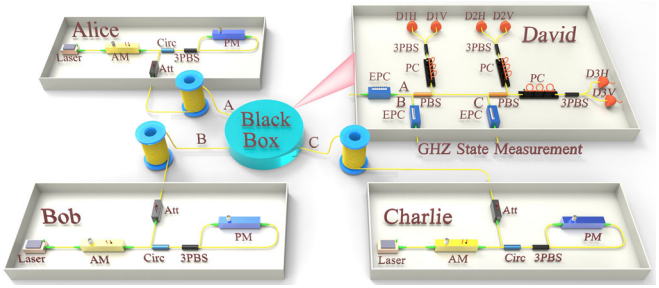

FIG. 1 (color online). Schematic layout of the MDI-QCC setup. AM: amplitude modulator used to prepare decoy states. 3PBS: 3-port polarization-maintaining PBS, which, besides the function of PBS, can transit optical pulses from fast axis to slow axis. Circ: circulator. PM: phase modulator, combining with 3PBS and Circ, is used to encode qubits. PC: polarization controller which makes a unitary transformation like a half-wave plate such that it corresponds to a 45° rotation of the polarization. Black box: the GHZ-state measurement device. Att: attenuator used to prepare weak coherent pulses. EPC: electric polarization controller used to adjust the frame of reference. PBS: polarizing beam splitter which transmits $|H\rangle$ and reflects $|V\rangle$ polarizations; $D1H$, $D2V$, $D2H$, $D2V$, $D3H$, and $D3V$: single-photon detectors.

$$R_{\mathrm{QCC}} = Q_v^Z + Q_{111}^Z[1 - H(e_{111}^{BX})] - H(E_{\mu\nu\omega}^{Z*}) f Q_{\mu\nu\omega}^Z, \quad (1)$$

where $Q_{\mu\nu\omega}^Z$ ($E_{\mu\nu\omega}^{Z*}$), the gain (quantum bit error rate) of Z basis, can be directly obtained from the experimental results. The subscript $\mu\nu\omega$ means that Alice, Bob, and Charlie send out phase-randomized weak coherent pulses with intensity μ, ν, and ω, respectively. Note that each of these pulses has single-photon state components and the ones of n (> 1) photons or zero photon. For the postselected GHZ states contributed solely by the single-photon state components, the gain Q_{111}^Z of Z basis and the bit error rate e_{111}^{BX} of X basis can be estimated by the decoy-state method. Q_v^Z is the gain that Alice sends out vacuum state component in Z basis and David obtains a GHZ state measurement result. Here, we assume that Alice's raw key is the reference raw key, the parameter f is the error correction efficiency ($f = 1.16$ in our simulation below), and $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. The information-theoretic security proof of MDI-QCC is shown in the Supplemental Material [23], from which we have $E_{\mu\nu\omega}^{Z*} = \max\{E_{\mu\nu\omega}^{ZAB}, E_{\mu\nu\omega}^{ZAC}\}$. Here, $E_{\mu\nu\omega}^{ZAB}$ ($E_{\mu\nu\omega}^{ZAC}$) is the quantum bit error rate of Z basis between Alice and Bob (Charlie).

In the same manner, the key generation rate of MDI-QSS in the asymptotic limit is given by

$$R_{\mathrm{QSS}} = Q_v^X + Q_{111}^X[1 - H(e_{111}^{BZ})] - H(E_{\mu\nu\omega}^{X}) f Q_{\mu\nu\omega}^X, \quad (2)$$

where $Q_{\mu\nu\omega}^X$ ($E_{\mu\nu\omega}^X$), the gain (quantum bit error rate) of X basis, can also be directly obtained from the experimental results. For the single-photon state contribution, the gain Q_{111}^X of X basis and bit error rate e_{111}^{BZ} of Z basis can be estimated by the decoy-state method. Q_v^X is the gain that Alice sends out vacuum state component in X basis and David obtains a GHZ state measurement result. However, the overall quantum bit error rate $E_{\mu\nu\omega}^X$ (always about 37.5% for arbitrarily-long transmission distances) in X basis is so high that it is virtually impossible to use weak coherent sources to perform MDI-QSS with Eq. (2). To solve the problem, in the Supplemental Material we propose, in detail, to use the triggered spontaneous parametric down conversion sources [35], or the conventional weak coherent state sources together with the quantum nondemolition measurement technique [36].

However, such a solution is disadvantageous as it requires experimentally challenging technology. Fortunately, we can exploit the extra classical bit information [37,38] to extract the raw key with little bit error rate (almost zero) so that we can implement MDI-QSS, again with weak coherent sources. The classical bit information corresponds to the information denoted by different overall phase regions over $[0, 2\pi)$ (the phase postselection technique). Meanwhile, we assume the gain and bit error rate of single-photon states to be in a uniform distribution over $[0, 2\pi)$ [38]. Therefore, the secure key rate of MDI-QSS with phase postselection can be given by (see Supplemental Material [23] for detail)

$$\tilde{R}_{\mathrm{QSS}} \geq \frac{1}{K^2} Q_{111}^X[1 - H(e_{111}^{BZ})] - H(\tilde{E}_{\mu\nu\omega}^X) f \tilde{Q}_{\mu\nu\omega}^X, \quad (3)$$

where K is the number of phase regions, $\tilde{Q}_{\mu\nu\omega}^X$ and $\tilde{E}_{\mu\nu\omega}^X$ are the gain and bit error rate of the pulses whose information is used to extract the raw key with little bit error rate. The phase postselection technique requires the sharing of a common phase reference [39] among users. A method for distributing such a phase reference is suggested in the Supplemental Material [23]. We note that the rigorous security of protocols involving phase postselection technique needs more investigations in the contexts of both QKD [37,38] and MDI-QSS.

To analyze the performance of the secret key rates of MDI-QCC and MDI-QSS, we present an analytical method with two decoy states to estimate the relevant parameters Q_{111}^Z, Q_{111}^X, e_{111}^{BZ}, and e_{111}^{BX}, which are required to be evaluated in Eqs. (1)–(3). In our simulation, we employ the following experimental parameters: the intrinsic loss coefficient β of the standard telecom fiber channel is 0.2 dB/km. For the threshold single-photon detectors, the detection efficiency $\eta_d = 40\%$, and the background count rate $p_d = 1 \times 10^{-7}$, as used in a recent decoy-state MDI-QKD experiment [40]. As a comparison, we also use the state-of-the-art single-photon detectors [41], with $\eta_d = 93\%$ and $p_d = 1 \times 10^{-7}$. Here, we neglect the overall misalignment-error probability of the system. The secure key rates of MDI-QCC with weak coherent sources in the cases of infinite decoy states and of the two decoy states are shown in Fig. 2(a). From the simulation result, we see that the estimation using two decoy states gives a secure key rate which is nearly the same as the corresponding one using infinite decoy states. In the case of asymptotic data with two decoy states, the secure transmission distance between Alice and the middle node of MDI-QCC is about 190 km for the detection efficiency of 40% (210 km for the detection efficiency of 93%). The secure key rates of MDI-QSS with weak coherent sources based on overall phase postselection technique are shown in Fig. 2(b). In the case of asymptotic data with two decoy states, the secure transmission distance is about 130 km for the detection efficiency of 40% (150 km for the detection efficiency of 93%) between the middle node and any user.

The information-theoretic security of our multiparty quantum communication protocols is guaranteed by the GHZ entanglement purification technique [22] though the security of MDI-QSS is complicated by phase postselection and needs further study. Indeed, the purpose of QCC and QSS protocols can be recognized as a procedure for Alice, Bob, and Charlie to share almost perfect GHZ states. Qualitatively, the more perfect the GHZ entanglement shared by Alice, Bob, and Charlie is, the more negligible

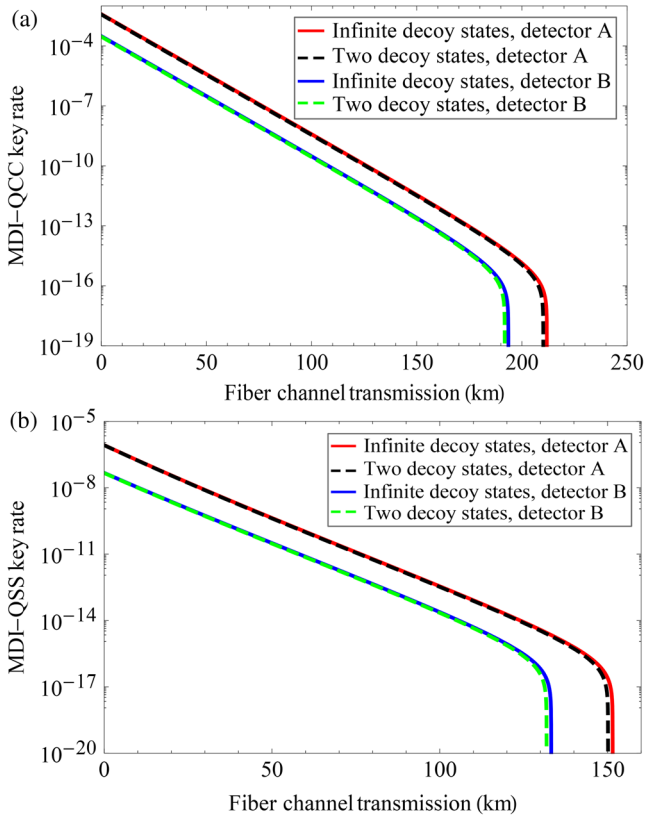

FIG. 2 (color online). Lower bound on the secure key rates versus fiber channel transmission. (a) MDI-QCC with weak coherent sources. (b) MDI-QSS with weak coherent sources based on phase postselection technique ($K = 8$). We show the simulation results of infinite decoy states and two decoy states with detector A (B) of detection efficiency 93% (40%), respectively. The phase-randomized weak coherent sources with (without) the phase postselection technique are used for MDI-QSS (MDI-QCC). The intensity of the signal state and one decoy state is 0.4 and 0.005 (0.11 and 0.005), while the other decoy state is a vacuum state in MDI-QCC (MDI-QSS).

the information would have been leaked to Eve [42]. It is thus of vital importance to quantify the quality of the GHZ entanglement. For this purpose, Alice, Bob, and Charlie independently and randomly prepare quantum states with phase-randomized weak coherent pulses in two complementary bases (X basis and Y basis) and then send to David, who performs the GHZ-state ($|\Phi_0^+\rangle$) measurement. What we take into consideration here is the postselected GHZ states contributed solely by the single-photon state components. This contribution can be estimated by the decoy-state method. For the GHZ entangled state $|\Phi_0^+\rangle$, local realistic theories must obey Mermin's inequality [14]:

$$M_{111} \equiv \langle XXX\rangle_{111} - \langle XYY\rangle_{111} - \langle YXY\rangle_{111} - \langle YYX\rangle_{111} \leq 2. \quad (4)$$

Here M_{111} is defined as the Mermin value and witnesses the quality of the GHZ entanglement; $\langle XXX\rangle_{111}$ and so on are the expectation values with respect to the GHZ states solely contributed by the single-photon state components. It is important to ensure that one only selects a single ensemble corresponding to the successful projection onto the GHZ state $|\Phi_0^+\rangle$. In our postselected GHZ states, the Mermin value, whose maximal value is 4 as predicted by quantum mechanics for ideal GHZ states, can reach about 3.5 as shown in Fig. 3 over the distribution distance of about 170 km from David to Alice (Bob, Charlie); more details can be found in the Supplemental Material [23]. This indicates that high-quality GHZ entanglement can be generated at this distance by the protocol. The proposed protocol can be regarded as a variance of the usual GHZ experiment testing local realism, namely, a time-reversed GHZ experiment where the state preparations replace the state measurements in the usual GHZ test. The interpretation of such a variance and, particularly, its relevance to the test of hidden-variable theories are interesting in its own right. We argue in the Supplemental Material [23] that such an experiment tests Mermin's argument [43] on the Kochen-Specker theorem [44].

In summary, we propose a feasible protocol for distributing the postselected GHZ entanglement and MDI multiparty quantum communication over a distance of more than 100 km for experimentally accessible parameter regimes. Combining the decoy-state and MDI protocols for QKD, we show that the information-theoretically secure MDI-QCC with the conventional weak coherent state sources can be implemented over a distance of about 190 km, as well as the MDI-QSS with weak coherent sources based on phase postselection technique over a distance of about 130 km. These distances are significantly beyond what one could expect previously for multiparty quantum communication with the GHZ entanglement. Our proposal thus suggests an

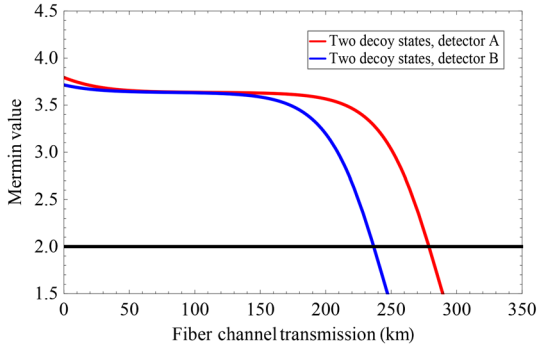

FIG. 3 (color online). The Mermin value M_{111} versus fiber channel transmission. We use two decoy states to estimate M_{111}. We show the simulation results for detector A (B) of detection efficiency of 93% (40%) in red (blue) solid curve, respectively. The overall misalignment-error probability e_d of the system is 1.5%, with other parameters identical to Fig. 2(a). We also show the line of constant 2, which is the maximal value allowed by local realism.

important avenue for practical long-distance multiparty quantum communication. The extension of our scheme to more legitimate users is straightforward.

We are grateful to the anonymous referees for their valuable comments and suggestions to improve the quality of the paper. This work has been supported by the CAS, the NNSF of China under Grant No. 61125502, and the Science Fund of Anhui Province for Outstanding Youth.

Y. F. and H.-L. Y. contributed equally to this work.

*zbchen@ustc.edu.cn

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski, Rev. Mod. Phys. **84**, 777 (2012).
[4] H. Shibata, T. Honjo, and K. Shimizu, Opt. Lett. **39**, 5078 (2014).
[5] J. Yin *et al.*, Nature (London) **488**, 185 (2012); X.-S. Ma *et al.*, Nature (London) **489**, 269 (2012).
[6] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).
[7] K. Chen and H.-K. Lo, Quantum Inf. Comput. **7**, 689 (2007).
[8] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[9] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[10] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001); Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **95**, 200502 (2005); S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007); C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
[11] B. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, Nat. Commun. **5**, 5480 (2014).
[12] M. Żukowski, A. Zeilinger, M. A. Horne, and H. Weinfurter, Acta Phys. Pol **A93**, 187 (1998).
[13] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989), pp. 69–72.
[14] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[15] C. Erven *et al.*, Nat. Photonics **8**, 292 (2014).
[16] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[17] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012); S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[18] S. Wiesner, SIGACT News **15**, 78 (1983).
[19] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).
[20] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[21] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999); P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000); H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
[22] E. N. Maneva and J. A. Smolin, Contemp. Math. **305**, 203 (2002); C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996); W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
[23] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.114.090501, which includes Refs. [24-32], for details.
[24] C.-Y. Lu, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **103**, 020501 (2009).
[25] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013).
[26] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
[27] Y. Liu *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).
[28] S.-B. Cho and Tae-Gon Noh, Opt. Express **17**, 19027 (2009); Y. Liu *et al.*, Phys. Rev. Lett. **109**, 030501 (2012); A. Cuevas, G. Carvacho, G. Saavedra, J. Cariñe, W. A. T. Nogueira, M. Figueroa, A. Cabello, P. Mataloni, G. Lima, and G. B. Xavier, Nat. Commun. **4**, 2871 (2013).
[29] T. Scheidl *et al.*, Proc. Natl. Acad. Sci. U.S.A. **107**, 19708 (2010).
[30] Z.-B. Chen, J.-W. Pan, Y.-D. Zhang, Č. Brukner, and A. Zeilinger, Phys. Rev. Lett. **90**, 160408 (2003).
[31] A. Peres, J. Mod. Opt. **47**, 139 (2000).
[32] X.-S. Ma *et al.*, Nat. Phys. **8**, 479 (2012).
[33] J.-W. Pan and A. Zeilinger, Phys. Rev. A **57**, 2208 (1998).
[34] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[35] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[36] P. Grangier, J. A. Levenson, and J.-P. Poizat, Nature (London) **396**, 537 (1998); A. Mizutani, K. Tamaki, R. Ikuta, T. Yamamoto, and N. Imoto, Sci. Rep. **4**, 5236 (2014).
[37] X. Ma and N. Lütkenhaus, Quantum Inf. Comput. **12**, 0203 (2012).
[38] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[39] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **89**, 062305 (2014); J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **90**, 042335 (2014); V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).
[40] Y.-L. Tang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).
[41] F. Marsili *et al.*, Nat. Photonics **7**, 210 (2013).
[42] B. M. Terhal, IBM J. Res. Dev. **48**, 71 (2004).
[43] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).
[44] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967).