Quantum key distribution using qudits that each encode one bit of raw key

H. F. Chau*

Department of Physics and Center of Theoretical and Computational Physics, Pokfulam Road, Hong Kong

(Received 14 July 2015; published 11 December 2015)

All known qudit-based prepare-and-measure quantum key distribution (PMQKD) schemes are more error resilient than their qubit-based counterparts. Their high error resiliency comes partly from the careful encoding of multiple bits of signals used to generate the raw key in each transmitted qudit so that the same eavesdropping attempt causes a higher bit error rate (BER) in the raw key. Here I show that highly-error-tolerant PMQKD schemes can be constructed simply by encoding one bit of classical information in each transmitted qudit in the form $(|i\rangle \pm |j\rangle)/\sqrt{2}$, where $|i\rangle$'s form an orthonormal basis of the 2^n-dimensional Hilbert space. Moreover, I prove that these schemes can tolerate up to the theoretical maximum of a 50% BER for $n \geqslant 2$ provided the raw key is generated under a certain technical condition, making them extremely-error-tolerant PMQKD schemes involving the transmission of unentangled finite-dimensional qudits. This shows the potential of processing quantum information using lower-dimensional quantum signals encoded in a higher-dimensional quantum state.

DOI: 10.1103/PhysRevA.92.062324 PACS number(s): 03.67.Dd, 03.65.Aa, 03.67.Hk, 89.70.−a

Introduction. Quantum key distribution (QKD) allows two cooperative players, Alice and Bob, to share a secret key whose security is guaranteed by the laws of quantum mechanics. Since the discovery of the first QKD scheme by Bennett and Brassard [1], researchers have been studying different aspects of QKD. New QKD protocols that are either more practical, efficient, or error tolerant have been proposed. Actual QKD experiments for some of the protocols have been carried out. Unconditional security proofs, including those covering realistic settings like the use of imperfect sources and detectors, for many of these protocols have been found. (See, for example, the review article in Ref. [2] for an overview.)

One line of research is to investigate the use of qudits rather than qubits as quantum information carriers in the QKD. In particular, Chau proved the unconditional security of a prepare-and-measure quantum key distribution (PMQKD) scheme (called Chau05) using 2^n-dimensional quantum particles as information carriers, each encoding n bits of the raw key [3]. Although his scheme has a very low key rate and is hard to implement using current technology, it can tolerate a bit error rate (BER) of up to 50% in the limit of $n \to +\infty$ [4]. This demonstrates the superior error-tolerant capability of the qudit-based PMQKD scheme as the best qubit-based PMQKD scheme known to date can only tolerate up to about 27.4% BER [5]. Recently, Sasaki *et al.* proposed a radically different qudit-based PMQKD scheme known as the round-robin differential-phase-shift (RRDPS) protocol in which Alice encodes multiple bits s_i in each of the N-dimensional qudit state as

$$\frac{1}{\sqrt{N}} \sum_{i=1}^{N} (-1)^{s_i} |i\rangle \tag{1}$$

so that Bob's measurement can only reveal one of the $(s_i - s_j)$'s of his choice [6]. This is a conceptually important scheme for it demonstrates that the security of the QKD need not link to the Heisenberg uncertainty principle [7]. In terms of performance, the RRDPS protocol can also tolerate up to a 50% BER in the $N \to +\infty$ limit. In addition, if the BER of the raw key is low, the key rate of the RRDPS protocol is much higher than that of Chau05. Several proof-of-principle experiments for the RRDPS protocol have been conducted [8–10].

Here I report a family of qudit-based PMQKD schemes whose security comes from a different principle. In these schemes, Alice and Bob randomly and independently prepare and measure qubitlike states, each in the form $(|i\rangle \pm |j\rangle)/\sqrt{2}$ in a 2^n-dimensional Hilbert space for $n \geqslant 2$ so that only one bit of the raw key is encoded and transmitted in the phase of each qudit state. (Here $|i\rangle$'s form an orthonormal basis of the 2^n-dimensional Hilbert space.) The security originates from the fact that the eavesdropper Eve has a hard time reading out a sizable portion of the raw key without being caught because she does not know the preparation basis of each qudit at the time when the quantum state is passing through the insecure channel under her control. By identifying $|i\rangle$ as the single-photon state in the ith optical pulse, these schemes have the additional attractive feature that the prepared states, which are essentially qubit states in diagonal basis, can be easily created and measured using a standard optical interferometer with variable path length. [Interestingly, the experimental techniques used to prepare quantum states in expression (1) in Refs. [8–10] can be adapted to prepare the states $(|i\rangle \pm |j\rangle)/\sqrt{2}$.] Using an aggressive entanglement distillation procedure involving local operation and two-way classical communications (LOCC2) originally reported in Ref. [5], I prove that Alice and Bob could share a provably secure secret key whenever the BER is less than 50% provided that the raw key obeys the technical condition to be stated in Eq. (2) later in the text, making it a family of PMQKD schemes that saturates the theoretical maximum limit of the tolerable BER using unentangled finite-dimensional quantum information carriers. This opens up the study of processing quantum information through the use of lower-dimensional quantum states embedded in a higher-dimensional Hilbert

*hfchau@hku.hk

Published by the American Physical Society under the terms of the Creative Commons Attribution 3.0 License. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

space or transferred through a higher-dimensional quantum channel.

Schemes. Let me denote the finite field of $N \equiv 2^n$ elements by the Galois field GF(N) and consider the following family of schemes.

The family of PMQKD schemes.

(1) Alice randomly picks $i \neq j \in \mathrm{GF}(N)$. She secretly prepares a state in the form $(|i\rangle \pm |j\rangle)/\sqrt{2}$ and sends it to Bob through an insecure quantum channel.

(2) Bob randomly picks $i' \neq j' \in \mathrm{GF}(N)$ and measures the state along $|i'\rangle \pm |j'\rangle$. He keeps his measurement outcome private.

(3) By announcing the pairs (i,j) and (i',j') through an unjammable classical channel, Alice and Bob establish a bit of raw key from those states with $(i,j) = (i',j')$. (They adopt the convention that $[|i\rangle + (-1)^s|j\rangle]/\sqrt{2}$ encodes the bit s.) They discard the measurement outcomes of those states with $(i,j) \neq (i',j')$. They repeat steps 1–3 until they have a long enough raw key.

(4) They estimate the BER of the raw key e_b, namely, the fraction of mismatched bits in their shared raw bit string, by comparing (and then discarding) a small random sample of the raw key. Using both accepted and rejected measurement outcomes in step 3, they calculate the conditional probability e_c that a state is prepared and measured as $(|i\rangle \pm |j\rangle)/\sqrt{2}$ given that it is prepared as $(|i\rangle \pm |j\rangle)/\sqrt{2}$ and measured as $[|(1-a)i + aj\rangle \pm |(a+1)j - ai\rangle]/\sqrt{2}$ for some $i,j,a \in \mathrm{GF}(N)$. [Note that all arithmetic in the state ket of a qudit is performed in the finite field GF(N) from now on.] They continue only if

$$e_b e_c + \frac{(N-1)(1-e_c)}{N-2} < \frac{1}{2}. \tag{2}$$

(5) Alice and Bob apply the following LOCC2 classical postprocessing procedure to the remaining raw key adapted from Ref. [5]. The values of the parameters k and r used in this procedure will be discussed later.

(a) Alice and Bob randomly group their corresponding bits in their remaining raw key in pairs. They reveal the parity of each corresponding pair and keep the first bit in those corresponding pairs whose parities agree. They repeat this process k times.

(b) Alice and Bob randomly group their corresponding bits in their remaining raw key in sets, each containing r bits. They replace each set by the parity of the r bits in the set.

(c) Alice and Bob obtain their final secret key by applying the Shor-Preskill privacy amplification procedure [5,11] to these bits using a Calderbank-Shor-Steane code that could correct up to, say, 1% quantum error.

Note that for the case of $N = 4$, the above scheme takes a rather simple form. Alice and Bob keep those states that are prepared and measured in diagonal basis of the same Hilbert subspace $\mathcal{H}_{ij} \equiv \mathrm{span}(|i\rangle, |j\rangle)$ for some $i \neq j \in \mathrm{GF}(4)$. In addition, e_c equals the length of the raw key divided by the total number of qudits that are prepared in the subspace $\mathcal{H}_{ij}$ and measured in either $\mathcal{H}_{ij}$ or $\mathcal{H}_{ab}$ subspaces, where i,j,a,b are the four distinct elements of GF(4).

Unconditional security proof. Now I show the unconditional security [12,13] of this family of PMQKD schemes for $N \geqslant 4$ by proving the unconditional security of the following associated family of entanglement-distillation-based quantum key distribution (EDQKD) protocols using the Shor-Preskill-type argument [11].

The associated family of EDQKD protocols.

(1) Alice prepares the state $\sum_{\ell \in \mathrm{GF}(2)} |\ell,\ell\rangle/\sqrt{2}$. She randomly picks $\lambda,\beta \in \mathrm{GF}(N)$ with $\lambda \neq 0$ and applies the linear transformation

$$L_{\lambda\beta}|a\rangle = |\lambda a + \beta\rangle \tag{3}$$

for all $a \in \mathrm{GF}(N)$ to the second qudit. She keeps the first qudit and sends the second qudit to Bob through an insecure quantum channel.

(2) Bob randomly picks $\lambda',\beta' \in \mathrm{GF}(N)$ with $\lambda' \neq 0$ and applies $L^{-1}_{\lambda'\beta'}$ to the qudit he received from Alice. Then Alice and Bob projectively measure their shared state along the basis

$$\mathcal{B} = \{|\Psi_{a\ell}\rangle : a \in \mathrm{GF}(N), \ell \in \mathrm{GF}(2)\}, \tag{4}$$

where $|\Psi_{a\ell}\rangle \equiv [|0,a\rangle + (-1)^\ell |1,a+1\rangle]/2$. They keep those states in the form $|\Psi_{\kappa\ell}\rangle$ with $\kappa \in \mathrm{GF}(2)$ (which are regarded as qubit pairs from now on) provided $\lambda = \lambda'$ and $\beta = \beta'$. They repeat steps 1 and 2 until they have a sufficient number of shared qubits.

(3) Let $e_{a\ell}$ be the conditional probability that the joint measurement outcome in step 2 is $|\Psi_{a\ell}\rangle$ given that $\lambda = \lambda'$ and $\beta = \beta'$. They continue only if

$$e_{01} + e_{11} + (N-1)(e_{10} + e_{11}) < \tfrac{1}{2}. \tag{5}$$

(4) Alice and Bob perform the following entanglement purification procedure adapted from Ref. [5].

(a) They randomly group their corresponding qubits in tetrads, where each tetrad consists of two pairs shared by them. Alice applies the unitary operation $|\psi_\kappa,\psi_\ell\rangle \mapsto |\psi_\kappa,\psi_{\kappa+\ell}\rangle$ to her share of the particles in the tetrad, where $|\psi_\kappa\rangle \equiv [|0\rangle + (-1)^\kappa|1\rangle]/\sqrt{2}$; Bob does the same to his corresponding particles in the tetrad. Alice and Bob keep their second qubit pair if the measurement results of their first qubit pair in the diagonal basis $\mathcal{B}^\times \equiv \{\psi_0,\psi_1\}$ agree. They repeat this process k times.

(b) They randomly group their remaining qubits in sets, each with r shared qubit pairs. They separately apply the $[r,1,r]$ majority-vote error correction code for the rectilinear basis to their share of the qubits in each set.

(c) They apply a Calderbank-Shor-Steane code that could correct up to a 1% quantum error of the remaining shared quantum state to distill out almost perfect $|\Psi_{00}\rangle$ Einstein-Podolsky-Rosen pairs. Finally, by measuring each qubit of these states along the diagonal basis $\mathcal{B}^\times$ Alice and Bob obtain their secret key.

Clearly $|\Psi_{a\ell}\rangle = (I \otimes \mathtt{X}_a\mathtt{Z}^\ell)|\Psi_{00}\rangle$, where

$$\mathtt{X}_a|b\rangle = |a+b\rangle, \quad \mathtt{Z}|b\rangle = (-1)^{\mathcal{N}(b)}|b\rangle \tag{6}$$

for all $b \in \mathrm{GF}(N)$. Here $\mathcal{N}(b) = b^{N-1}$ is the norm of b [14]. Note that $N(0) = 0$ and $N(b) = 1$ if $b \neq 0$. Consider the expression

$$\begin{aligned}&\left(I \otimes L^{-1}_{\lambda\beta}\mathtt{X}_a\mathtt{Z}^\ell L_{\lambda\beta}\right)|\Psi_{b\kappa}\rangle \\ &\quad = \sum_{\nu \in \mathrm{GF}(2)} (-1)^{\kappa\nu + \ell\mathcal{N}(\lambda(\nu+b)+\beta)}|\nu,\nu+b+\lambda^{-1}a\rangle\end{aligned} \tag{7}$$

for all $\lambda \neq 0, \beta, a, b \in \mathrm{GF}(N)$ and $\ell, \kappa \in \mathrm{GF}(2)$. Up to an irrelevant global phase, the right-hand side of Eq. (7) equals $|\Psi_{b+\lambda^{-1}a,\kappa'}\rangle$. Here $\kappa' = \kappa$ if $\ell = 0$ or $\mathcal{N}(\lambda b + \beta) = \mathcal{N}(\lambda(b + 1) + \beta)$; otherwise $\kappa' = \kappa + 1$. Hence, the sequences of probabilities of measurement outcome along $\mathcal{B}$ conditioned on different $\lambda = \lambda'$ and $\beta = \beta'$ in step 2 of the EDQKD protocol transform from one to another by permutation. In addition, all operations in step 4 except the final measurement in the diagonal basis permute elements in $\mathcal{B}$ up to an irrelevant phase. Therefore, Alice (Bob) may push the final measurement in $\mathcal{B}^{\times}$ in step 4c forward in time to immediately after step 1 (2) [5,15]. By renaming $\lambda = j - i$ and $\beta = i$, I get $L_{\lambda\beta}|0\rangle = |i\rangle$ and $L_{\lambda\beta}|1\rangle = |j\rangle$. Consequently, this EDQKD protocol is reduced to the PMQKD scheme. Furthermore, the Shor-Preskill argument implies that the unconditional security of the above PMQKD scheme follows that of the EDQKD protocol [11].

I now proceed to analyze the security of the EDQKD protocol. Clearly, the probabilities $e_{a\ell}$ obey $\sum_{a\in\mathrm{GF}(N),\ell\in\mathrm{GF}(2)} e_{a\ell} = 1$. Since λ and β are randomly chosen for each transmitted qudit and are unknown to Eve during the transmission, Eq. (7) implies that

$$e_{a0} + e_{a1} = e_{b0} + e_{b1} \tag{8}$$

for all nonzero $a, b \in \mathrm{GF}(N)$. So, if Eq. (5) is satisfied, $e_{00} > 1/2$ is the greatest element among the $e_{a\ell}$'s. Furthermore, by comparing the definitions of e_b and e_c in step 4 of the PMQKD schemes with the definitions of the $e_{a\ell}$'s in step 3 of the EDQKD protocols, I find the following correspondences:

$$e_b e_c = (e_{01} + e_{11}), \tag{9}$$

$$e_c = e_{00} + e_{10} + e_{01} + e_{11}, \tag{10}$$

and

$$1 - e_c = (e_{10} + e_{11})(N - 2). \tag{11}$$

Thus, Eq. (5) implies Eq. (2).

The probabilities that the joint measurement outcomes for those remaining shared qubits just before step 4 of the EDQKD protocol can be written as the elements of the 2×2 error matrix

$$\begin{pmatrix} p_I & p_z \\ p_x & p_y \end{pmatrix} \equiv \frac{1}{e_c}\begin{pmatrix} e_{00} & e_{01} \\ e_{10} & e_{11} \end{pmatrix}. \tag{12}$$

By treating each pair of shared qudits as a shared qubit pair, then p_I, p_x, p_y, and p_z can be regarded as the probabilities that Bob's share of the qubit pair has suffered I, σ_x, σ_y, and σ_z errors, respectively.

Note that in the above EDQKD protocol, step 4 is analogous to a similar procedure in Ref. [5] with the roles of X and Z errors being swapped. That is to say, step 4a is a variation of the BXOR test [16,17] that reduces the Z error of the resultant qubit pairs, whereas step 4b reduces the X error. Applying Proposition 1 in Ref. [5] with the roles of X and Z errors exchanged, the corresponding error matrix for the shared qubits immediately after step 4a equals

$$\begin{pmatrix} p_I^{k\mathrm{EP}} & p_z^{k\mathrm{EP}} \\ p_x^{k\mathrm{EP}} & p_y^{k\mathrm{EP}} \end{pmatrix} = \frac{1}{2(A + C)}\begin{pmatrix} A + B & C + D \\ A - B & C - D \end{pmatrix}, \tag{13}$$

where $A = (p_I + p_x)^{2^k}$, $B = (p_I - p_x)^{2^k}$, $C = (p_y + p_z)^{2^k}$, and $D = (p_y - p_z)^{2^k}$. Since $e_{00} > 1/2$, so is p_I. Hence from Proposition 2 in Ref. [5] (again with X and Z errors exchanged), the quantum error rate of the shared qubits can be reduced to less than 1% after step 4b and therefore almost perfect $|\Psi_{00}\rangle$'s can be distilled in step 4c if the r in step 4b equals $0.005/(p_y^{k\mathrm{EP}} + p_z^{k\mathrm{EP}})$ and $2r(1/2 - p_x^{k\mathrm{EP}} - p_y^{k\mathrm{EP}})^2 \gg 1$. Such an r exists if $(B + D)^2 \gg 400C(A + C)$. Since $p_I > 1/2$, $p_I - p_z > p_x - p_y$. Thus, r exists by picking a sufficiently large k as long as

$$(p_I - p_x)^2 > (p_I + p_x)(p_y + p_z). \tag{14}$$

(Incidentally, the same condition has been proven in Ref. [5] for the special case of $p_x = p_y = p_z$.) From Eqs. (9) and (12) plus the fact that $e_{00} + e_b e_c + (N - 1)(1 - e_c)/(N - 2) - e_{11} = 1$, the sufficient condition for the existence of r can be rewritten as

$$f(e_b, e_c, e_{11}) = \left[1 - e_b e_c - \frac{N(1 - e_c)}{N - 2} + 2e_{11}\right]^2 - e_b(1 - e_b)e_c^2 > 0. \tag{15}$$

The maximum tolerable BER $e_{\max}$ of the EDQKD protocol and hence the PMQKD scheme is the largest possible e_b provided that the parameters e_b, e_c, e_{11} pass the test in step 3 of the EDQKD protocol. That is, $e_{\max} = \sup\{e_b : f(e_b, e_c, e_{11}) > 0\, \forall e_c, e_{11}; (e_b, e_c, e_{11}) \in \mathcal{R}\}$, where $\mathcal{R} = \{(e_b, e_c, e_{11}) \in [0,1]^3 : e_b e_c + (N - 1)(1 - e_c)/(N - 2) < 1/2\}$. Since f is quadratic in e_b, e_c, and e_{11}, the value of $e_{\max}$ can be calculated readily. Specifically, elements in $\mathcal{R}$ obey $1 - e_b e_c - N(1 - e_c)/(N - 2) > 0$. So, $f(e_b, e_c, e_{11}) \geqslant f(e_b, e_c, 0)$ for all $(e_b, e_c, e_{11}) \in \mathcal{R}$. Moreover, for any fixed $e_b \in [0, 1/2)$ and by varying e_c in $\mathcal{R}$, it is straightforward to see that $f(e_b, e_c, 0)$ is minimized when $e_c = e_c^*(e_b) \equiv N/\{2[N - 1 - (N - 2)e_b]\}$. Finally, it is easy to check that $f(e_b, e_c^*(e_b), 0) > 0$ if and only if $e_b \in [0, 1/2)$ provided $N \geqslant 4$. In summary, for $(e_b, e_c, e_{11}) \in \mathcal{R}$, $f(e_b, e_c, e_{11}) > 0$ whenever $e_b < 1/2$. In addition, $f \to 0$ as $e_{11} = 0$, $e_b \to 1/2$, and $e_c \to 1$. Therefore, $e_{\max} = 1/2$; this can be attained when Eve feeds every particle sent by Alice through a completely dephasing channel before giving it to Bob. By the standard composability definition of security for the QKD [12,13], the family of EDQKD protocols for $N \geqslant 4$ can therefore produce a shared secret key whenever the BER is less then 50%.

To conclude, using the above family of PMQKD schemes, Alice and Bob can establish a secure key whenever the BER of the raw key is less than 50% provided $N \geqslant 4$ and the accepted data rate e_c obeys Eq. (2). Since it is impossible to recover any encoded classical message after sending through a binary symmetric channel with crossover probability 1/2, this family of PMQKD schemes shows that an extremely-error-tolerant QKD scheme (as measured by its tolerable BER) can be constructed by sending four-dimensional qubitlike qudits, each containing a single bit of classical information encoded in its phase. (Another extremely-error-tolerant scheme of this type using four-dimensional qudits before this study was Chau05, which can distill a secret key up to a 35.6% BER.) The security of this family of schemes comes partly from the ability to deduce the X-error rate through a clever use of the accepted data rate e_c in step 4. This opens up additional possibilities

for doing quantum information processing through carefully designed algorithms that send lower-dimensional quantum states through a higher-dimensional channel.

Outlook. So far, the analysis is restricted to the case of an ideal source and detectors in the arbitrarily long raw key length limit. One still needs to investigate the security and performance of this family of schemes for realistic sources (say, by a decoy state method [18–20]) and detectors (say, by measurement-device-independent techniques [21,22]) in the finite-key-length setting [23–26] using one-way or two-way classical postprocessing.

Acknowledgments. I thank C.-H. F. Fung for his discussions, especially during the preliminary stage of this work. I also thank X. Ma for his discussions on the experimental implementation. This work was supported in part by the RGC Grant No. HKU8/CRF/11G of the Hong Kong SAR Government.

[1] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing* (IEEE, Piscataway, 1984), pp. 175–179, reprinted with typographic corrections in Theor. Comput. Sci. **560**, 7 (2014).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[3] H. F. Chau, IEEE Trans. Inf. Theory **51**, 1451 (2005).

[4] There is a subtlety in defining BER for qudits. See Ref. [3] for the precise definition in the case of Chau05.

[5] H. F. Chau, Phys. Rev. A **66**, 060302 (2002).

[6] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature (London) **509**, 475 (2014).

[7] M. Curty, Nat. Phys. **10**, 479 (2014).

[8] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **114**, 180502 (2015).

[9] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nat. Photon. **9**, 827 (2015).

[10] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nat. Photon. **9**, 832 (2015).

[11] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[12] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Theory Of Cryptography: Second Theory Of Cryptography Conference, TCC 2005*, edited by J. Killian, Lecture Notes in Computer Science Vol. 3378 (Springer, Berlin, 2005), pp. 386–406.

[13] R. Renner and R. König, in *Theory Of Cryptography: Second Theory Of Cryptography Conference, TCC 2005* (Ref. [12]), pp. 407–425.

[14] R. Lidl and H. Niederreiter, *Introduction To Finite Fields And Their Applications* (Cambridge University Press, Cambridge, 1994), p. 54.

[15] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[16] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[17] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[18] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[19] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[20] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[21] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[22] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).

[23] M. Hayashi, Phys. Rev. A **74**, 022307 (2006).

[24] C.-H. F. Fung, X. Ma, and H. F. Chau, Phys. Rev. A **81**, 012318 (2010).

[25] M. Hayashi and T. Tsurumaru, New J. Phys. **14**, 093014 (2012).

[26] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 1038 (2014).