Efficient quantum key distribution over a collective noise channel

Xi-Han Li,[1,2,3] Fu-Guo Deng,[1,3,4,*] and Hong-Yu Zhou[1,2,3]

[1]*The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, China*

[2]*Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, China*

[3]*Beijing Radiation Center, Beijing 100875, China*

[4]*Department of Physics, Applied Optics Beijing Area Major Laboratory, Beijing Normal University, Beijing 100875, China*

(Received 22 May 2008; published 13 August 2008)

We present two efficient quantum key distribution schemes over two different collective-noise channels. The accepted hypothesis of collective noise is that photons travel inside a time window small compared to the variation of noise. Noiseless subspaces are made up of two Bell states and the spatial degree of freedom is introduced to form two nonorthogonal bases. Although these protocols resort to entangled states for encoding the key bit, the receiver is only required to perform single-particle product measurements and there is no basis mismatch. Moreover, the detection is passive as the receiver does not switch his measurements between two conjugate measurement bases to get the key.

DOI: 10.1103/PhysRevA.78.022321 PACS number(s): 03.67.Pp, 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) has become one of the most important branches of quantum information. The principle of quantum mechanics was introduced into communication to ensure its security by Bennett and Brassard (BB84) in 1984 [1], which started the vigorous development of quantum communication. Different from classic communication, the security of quantum communication is based on the laws of physics rather than the difficulty of computation. The eavesdropper Eve is so powerful that her ability is only limited by the principles in quantum mechanics. However, the noncloning theorem forbids Eve to eavesdrop the quantum signals freely and fully as her action will inevitably disturb the unknown states and leave a trace in the outcomes obtained by the two legitimate users. By far, QKD has attracted the most attention [2–10].

Photons are popular entities for quantum communication since they are fast, cheap, easy to control, and interact weakly with environment. QKD experiments through free air and optical fibers have been demonstrated over the past 20 years [11–13]. It is found in the experimental results that the polarization of photons is incident to be influenced by the thermal fluctuation, vibration, and the imperfection of the fiber, which are generally called noise. Both the inhomogeneity of atmosphere in a free space and the birefringence in an optical fiber are obstacles to the application of quantum communication with photon polarization degrees of freedom. The noise not only changes the fidelity of quantum states carrying the information, which will decrease the successful probability of schemes consequently, but also gives the eavesdropper a chance to disguise her disturbance with a better fiber, which will directly impact the key point of quantum communication, i.e., its security. The most obvious solution is to continuously estimate the transformation caused by the noise and compensate for it momentarily. This can be denoted as a feedback control project. However, this method is difficult in practice and it requires an interruption of transmission. If the fluctuation is too fast, the method is invalid.

There are two valid methods to solve this problem: one is choosing another degree of freedom to encode the key bits, and the other is first to theorize the noise and then find a way to remove or decrease the noise effect. The typical solution of finding a new degree of freedom is phase coding, which has been demonstrated in optical fibers experimentally [12]. Although most of the apparatus in the experiment was polarization-dependent, while the polarization of the photon would be influenced by the birefringence effect, the Faraday orthoconjugation effect [14] was proposed to circumvent this problem. However, the phase-based schemes require complex interferometers and high precision timing. Moreover, some phase coding protocols are two-way communications that are susceptive to Trojan horse attack [5,15]. The second method is first constructing an appropriate noise model, and then finding a resolvent accordingly, such as quantum error correct code (QECC) [16], single-photon error rejection [17,18], quantum error-rejection code with two qubits [19–21], and decoherence-free subspace (DFS) [22–24]. The QECC encodes one logical bit into several physical qubits according to the type of noise, and then the users measure the stabilizer codes to detect errors and correct them. For single-photon error rejection schemes and protocols utilizing the idea of DFS, there is an important precondition called the collective noise assumption [25]. That is, the photons travel inside a time window that is shorter than the variation of noise. In other words, if several qubits transmit through the noise channel simultaneously or they are close to each other spatially, the transformation of the noise on each of the qubits is identical.

The single-photon error rejection schemes transmit photons faithfully without ancillary qubits through a collective noise channel. The two parts of the photon split by a polarizing beam splitter (PBS) are adjusted to have a time delay, and then they suffer from the same noise consecutively. The

*fgdeng@bnu.edu.cn

effect of noise is canceled by selecting the final state arriving at a special time slot. In other words, the state collapses into a subspace that is not impacted by the noise with a certain probability. Kalamidas proposed a single-photon error rejection protocol in 2005 [17], which is efficient and convenient except for the use of Pockels cells (PC). Recently, we presented a single-photon transmission scheme with linear optics against collective noise [18], in which only passive linear optical elements are required. In a sense, the schemes using only single-photon states to reject errors can be regarded as a kind of DFS scheme in which the time degree of freedom is introduced to form the DFS with the two polarization parts.

The DFS can be made up of several qubits which experience the same noise and compensate the effect of noise to implement a fault-tolerance communication. Walton *et al.* proposed a QKD scheme using the idea of DFS in 2003 [22]. In their scheme, the logical qubit is encoded into two time-bin qubits to protect the quantum system against a collective-dephasing noise. The Hilbert space is extended by the time degree of freedom, so that the receiver could perform his measurement with a fixed basis. Later, Boileau *et al.* presented a QKD protocol with a collective random unitary error model by using the linear combinations of two singlet states $|\psi^-\rangle$, which are invariant under whatever rotations [23]. The spatial degree of freedom is also introduced to distinguish the states. However, the receiver has to discard half of the samples due to the inconclusive results, similar to traditional QKD protocols such as the BB84 QKD protocol in which the two legitimate users abandon half of the outcomes owing to wrong measurement bases. Recently, Wang proposed a robust QKD using a subspace of two-qubit states [24]. The states being transformed out of the subspace by the collective rotation are rejected by a parity check and then the total error rate in the QKD protocol decreases.

In this paper, we present two fault-tolerant quantum key distribution schemes against collective noises. One is used against a collective-dephasing noise and the other is used against a collective-rotation noise. The DFS is spanned by two entangled states, and the spatial and polarization degrees of freedom are both introduced. The receiver uses passive detection, i.e., he is not required to switch between conjugate measurements, to obtain the related outcomes. The most important merit of these two schemes is that there is no basis mismatch, which means there is no abandonment of samples owing to wrong basis measurement in these two schemes.

II. QUANTUM KEY DISTRIBUTION AGAINST A COLLECTIVE NOISE

We select special Bell states according to the form of noise to build blocks for constructing a decoherence-free subspace. The key bits are encoded on the states and the relative order of the photon pairs.

A. QKD against a collective-dephasing noise

A collective-dephasing noise can be described as

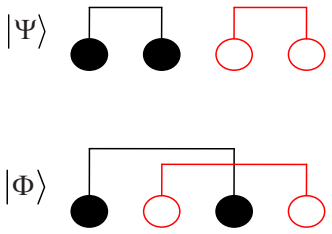

FIG. 1. (Color online) Schematics of the two spatial bases. Lines represent the entanglement between particles.

$$U|0\rangle = |0\rangle, \quad U|1\rangle = e^{i\phi}|1\rangle, \tag{1}$$

where ϕ is the parameter of the noise and it fluctuates with time. Generally, the logical qubit encoded into two physical qubit product states in the following is immune to this collective-dephasing noise as the two logical qubits acquire the same phase factor $e^{i\phi}$,

$$|0\rangle_L = |01\rangle, \quad |1\rangle_L = |10\rangle, \tag{2}$$

where the subscript L represents the logical bit, and $|0\rangle$ and $|1\rangle$ represent the horizontal polarization state and the vertical one, respectively, which are the two eigenstates of Pauli operator σ_z (Z basis). We choose two superpositions of these two logical bits to form a DFS. They are two antiparallel Bell states written as

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \tag{3}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{4}$$

Generally speaking, a secure QKD protocol needs at least two nonorthogonal measuring bases. The eavesdropper cannot obtain the information directly and will disturb the quantum state without the knowledge of its basis information. However, the use of two nonorthogonal bases results in the abandonment of half instances measured by the receiver with wrong bases, or calls for the technique of quantum storage, which is difficult at present. For constructing an efficient QKD protocol, we pack two two-particle entangled states as one group and introduce the spatial degree of freedom to form the nonorthogonality. The spatial degree of freedom means the relative orders of the four particles. Two permutations are used to form the two spatial bases to prepare the quantum states, shown in Fig. 1. They are the neighboring basis $|\Psi\rangle$ in which the two entangled particles are in close proximity, and the crossing basis $|\Phi\rangle$ in which particles of the two entangled states are ranged alternately.

The four states with which we encode the logical bits can be written as

$$\Psi_0^{dp} = |\psi^+\rangle_{12} \otimes |\psi^+\rangle_{34}, \tag{5}$$

$$\Psi_1^{dp} = |\psi^-\rangle_{12} \otimes |\psi^-\rangle_{34}, \tag{6}$$

$$\Phi_0^{dp} = |\psi^+\rangle_{13} \otimes |\psi^+\rangle_{24}, \tag{7}$$

$$\Phi_1^{dp} = |\psi^-\rangle_{13} \otimes |\psi^-\rangle_{24}. \tag{8}$$

Here the subscripts 0 and 1 on the left side represent the key bits encoded, and subscripts {1,2,3,4} on the right side denote the sequence of these four particles on the line of transmission. We can distinguish them by their time of arrival. Under the assumption of collective noise, the interval between the first and the fourth photons should be shorter than the fluctuation time of the noise parameter ϕ, which ensures that these four photons suffer from the same noise.

These four states in terms of the X basis $|\pm x\rangle$ are shown below, where $|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ are the two eigenstates of the Pauli operator σ_x. For the sake of simplicity, we use $|\pm\rangle$ representing $|\pm x\rangle$ in the following:

$$\Psi_0^{dp} = a + b, \tag{9}$$

$$\Psi_1^{dp} = c - d, \tag{10}$$

$$\Phi_0^{dp} = a + c, \tag{11}$$

$$\Phi_1^{dp} = b - d, \tag{12}$$

where

$$a = \frac{1}{2}(|+\,+\,+\,+\rangle + |-\,-\,-\,-\rangle)_{1234}, \tag{13}$$

$$b = \frac{1}{2}(|+\,+\,-\,-\rangle + |-\,-\,+\,+\rangle)_{1234}, \tag{14}$$

$$c = \frac{1}{2}(|+\,-\,+\,-\rangle + |-\,+\,-\,+\rangle)_{1234}, \tag{15}$$

$$d = \frac{1}{2}(|+\,-\,-\,+\rangle + |-\,+\,+\,-\rangle)_{1234}. \tag{16}$$

It is not difficult to verify that $\langle\Psi_0^{dp}|\Psi_1^{dp}\rangle = 0, \langle\Phi_0^{dp}|\Phi_1^{dp}\rangle = 0$, and $\langle\Phi_i^{dp}|\Psi_i^{dp}\rangle = \frac{1}{2}\,(i = 0, 1)$. For each basis Ψ^{dp} and Φ^{dp}, the receiver can distinguish the two states in a deterministic way with four single-particle measurements.

Now, let us describe the QKD scheme in detail as follows:

(S1) The sender Alice chooses a random $(n+2\delta)$ bit string K and a random $(n+2\delta)$ bit string B.

(S2) Alice encodes each bit of the key string K according to $\{|\Psi_0^{dp}\rangle, |\Psi_1^{dp}\rangle\}$ if the corresponding bit in the basis string B is 0, or encodes into $\{|\Phi_0^{dp}\rangle, |\Phi_1^{dp}\rangle\}$ if the corresponding bit in B is 1.

(S3) Alice sends the $(n+2\delta)$ four-particle states to the receiver Bob.

(S4) Bob performs the single-particle product measurements on each quartet after the receipt subsequently. He selects randomly 2δ states from the sequence for the eavesdropping check, where δ states are measured with the Z basis and the other δ samples are measured in the X basis. The residual n samples used to share the secret key are measured in the X basis. Bob records all of the measurement results.

(S5) Bob tells Alice the positions of groups chosen for the eavesdropping check and asks Alice for the initial states of these samples. After receipt of these messages, Bob checks the security of the transmission by estimating the error rate. If the error rate is acceptable, they continue to the next step. Otherwise, they abort the protocol.

(S6) After they affirm the security of the transmission, Alice announces B, with which Bob can determine the key bits. These results are taken as a raw key string. Error correction and privacy amplification are required to obtain the final key.

Except for the samples used for the security analysis with Z basis measurements, all the other photons are measured with the X basis. That means the receiver is not required to switch between conjugate measurement bases to get the message. And this scheme is efficient as with Alice's information of the basis, all the instances are used to generate the key, not just 1/4 of those in the QKD scheme against a collective-dephasing noise shown in Ref. [22]. Moreover, it does not require the receiver Bob to measure his photons with joint two-photon measurements, different from that in Ref. [22].

B. QKD against a collective-rotation noise

Another common noise model called collective unitary rotation noise satisfies

$$U_r|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,$$

$$U_r|1\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle. \tag{17}$$

The parameter θ depends on the noise in the quantum channel and fluctuates with time. With such a type of collective errors, we choose $|\psi^-\rangle$ and $|\phi^+\rangle$ to form the DFS, where

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{18}$$

They are invariant under this type of rotation. Similar to the method used above, we pack two entangled states as one group. Four combinations to code the key bits are

$$\Psi_0^r = |\phi^+\rangle_{12} \otimes |\phi^+\rangle_{34} = e + f, \tag{19}$$

$$\Psi_1^r = |\psi^-\rangle_{12} \otimes |\psi^-\rangle_{34} = g - h, \tag{20}$$

$$\Phi_0^r = |\phi^+\rangle_{13} \otimes |\phi^+\rangle_{24} = e + g, \tag{21}$$

$$\Phi_1^r = |\psi^-\rangle_{13} \otimes |\psi^-\rangle_{24} = f - h, \tag{22}$$

where

$$e = \frac{1}{2}(|0000\rangle + |1111\rangle)_{1234}, \tag{23}$$

$$f = \frac{1}{2}(|0011\rangle + |1100\rangle)_{1234}, \tag{24}$$

$$g = \frac{1}{2}(|0101\rangle + |1010\rangle)_{1234}, \tag{25}$$

$$h = \frac{1}{2}(|0110\rangle + |1001\rangle)_{1234}. \quad (26)$$

It is easy to find that the superposition terms of $\{\Phi_0^r, \Phi_1^r, \Psi_0^r, \Psi_1^r\}$ on the Z basis is similar to those of $\{\Phi_0^{dp}, \Phi_1^{dp}, \Psi_0^{dp}, \Psi_1^{dp}\}$ on the X basis. In this QKD protocol, the sender Alice prepares a sequence of quartet states randomly in $\Psi_0^r(\Phi_0^r)$ or $\Psi_1^r(\Phi_1^r)$ to denote the key bit 0 or 1. The choice of the basis for each state is stochastic. Then she sends the sequence to Bob. Bob chooses a sufficiently large subset of the multiplets as the checking samples and measures them with the measuring bases X and Z randomly. The other groups of states are measured with Z basis. Bob records all of the measurement results and tells Alice the positions of checking samples he selected. With Alice's information of the original states of these checking samples, Bob analyzes the error rate. If the error rate is reasonably low, they determine the channel is secure. Otherwise, they abandon their measurement results and repeat the communication from the beginning. After ensuring the security of transmission, Alice tells Bob the spatial bases she used to produce the quartets, with which Bob can deduce the key sequence from his measurement outcomes.

III. SECURITY ANALYSIS

For one-way quantum communication, there are two main means of eavesdropping. One is the intercept and resend attack [15] and the other is that using an auxiliary particle to interact with the particles carrying messages and measuring the auxiliary photon to get some useful information. The interaction can be two-particle unitary operation or controlled-NOT (CNOT) gate [16]. For simplicity, we denote the eavesdropping check by measuring samples with the X (Z) basis as the X (Z) check in the following.

Considering the first QKD scheme against a dephasing noise, as key bits are encoded into four-particle entangled states, the direct eavesdropping done by the eavesdropper Eve is the intercept-measure-resend attack. There are two kinds of measurements: the single-particle product measurements and the Bell-basis measurements. For this scheme, the receiver Bob can obtain the message only in the X basis. If her measurement outcome is a decomposition of a (d), Eve concludes that the key bit is 0 (1) directly. For other results, Eve cannot get the key until Alice publishes the information of spatial bases, Ψ^{dp} or Φ^{dp}. If she resends a fake product state to Bob according to her measurement results, the error rate in the X check is $e_X=0$ and the error rate in the Z check is $e_Z=75\%$. So the average error rate is $e_A=37.5\%$. There is another way to resend the fake state. The eavesdropper Eve guesses the original states according to her results and resends entangled fake states. From Eqs. (5)–(8), one can see that Eve will get a wrong state with a half opportunity, which will be discovered with probability 25% both in the X check and Z check. The average error rate of resending a guess state is 25%. The calculation of the error rate when Eve is measuring in the Bell basis is a little complex because of the quantum entanglement swapping phenomenon [26]. There is a half opportunity for Eve to choose the correct spatial basis.

TABLE I. The relation between the error rate and the eavesdropping attack on the QKD protocol against the dephasing noise.

Dephasing noise	e_X	e_Z	e_A
MB: X, resend: product state	0	75%	37.5%
MB: X, resend: entangled state	25%	25%	25%
MB: Bell, resend: entangled state	25%	12.5%	19.25%
CNOT gate on auxiliary on X basis	0	25%	12.5%

For a wrong basis, Eve can detect her mistake with 50% due to the appearance of $|\phi^{\pm}\rangle$ as results of entanglement swapping and then change the basis to prepare a fake state. This method will cause a 25% error rate in the X check and 12.5% in the Z check, while the average error rate is 19.25%. It is important to point out that with Bell-state measurements, Eve cannot get the key message until the bases are published by Alice. The error rates of some eavesdropping are shown in Table I.

From Eqs. (5)–(16), we find the parity of two particles in the X basis can reveal the key bit. For example, photons 3 and 4 are parallel in $|\Psi_0^{dp}\rangle$ and antiparallel in $|\Psi_1^{dp}\rangle$. Photons 2 and 4 are parallel in $|\Phi_0^{dp}\rangle$ and antiparallel in $|\Phi_1^{dp}\rangle$. The eavesdropper can utilize an auxiliary photon prepared in $|+\rangle_5$ to get the key message by means of two CNOT operators C_{35} and C_{45} along the x direction, where C_{ij} means using particle i as a control bit and j as a target bit. After the two CNOT gates, Eve measures photon 5 in the X basis. The outcome $|+\rangle$ ($|-\rangle$) means the two photons 3 and 4 are parallel (antiparallel) and the key bit is 0 (1). If Eve guesses the right spatial bases $|\Psi^{dp}\rangle$ or $|\Phi^{dp}\rangle$, her action will not be detected and she can get the key bit with the basis information. Otherwise, this method will introduce a 50% error rate in the Z check.

For the second QKD scheme, the calculation of error rates for different attacks is similar to the first one. A little difference is caused by the fact that the states used in the second protocol are symmetrical in the two measuring bases (MBs) X and Z. The error rates are listed in Table II. From these two tables, we find that the eavesdropper will introduce at least 12.5% error inevitably when she tries to wiretap. She will be detected by the two legitimate users. Eve can get half of the key bits both by X measurement and Z measurement with disturbing the unknown quantum states, but Alice will announce the preparation bases after the security check and the

TABLE II. The relation between the error rate and the eavesdropping attack on the QKD protocol against the rotation of polarization.

Polarization rotation	e_X	e_Z	e_A
MB: X, resend: product state	0	75%	37.5%
MB: X, resend: entangled state	25%	25%	25%
MB: Z, resend: product state	75%	0	37.5%
MB: Z, resend: entangled state	25%	25%	25%
MB: Bell, resend: entangled state	25%	25%	25%
CNOT gate on auxiliary on Z basis	25%	0	12.5%

key bit will be used to encrypt secret messages after they confirm its security. So this QKD protocol is secure in principle.

IV. DISCUSSION AND SUMMARY

Compared with the QKD scheme in Ref. [22], our first QKD scheme over a collective-dephasing noise channel has the advantage of having a higher intrinsic efficiency [30] as that in the former is 1/4 and almost all the instances in our scheme can be used to distill the private key. Moreover, this scheme requires the receiver Bob only to perform single-photon measurements for obtaining the outcomes used for distilling the private key and does not require him to switch the choice of the measuring bases, which will make the measurement simpler than that in Ref. [22]. On the other hand, in order to encode the states Ψ^{dp} and Φ^{dp}, the sender Alice needs to possess some modulators for spatial modes, which will increase the difficulty of the preparation of the logical qubit states. At present, Alice can exploit the similar apparatus composed of optical delays and switches in Ref. [7] to adjust the states Ψ^{dp} and Φ^{dp}. Also, Alice should prepare two EPR pairs for each logical state. Although this task can be accomplished at present by sending a pump pulse of ultraviolet light back and forth across a beta barium borate crystal [27,28], it is not in a practical application extensively.

Our second QKD scheme against a collective-rotation noise has a higher intrinsic efficiency than that in the robust polarization-based QKD scheme [23] as almost all the instances in our scheme can be used to create the private key and about 1/4 of the instances in the latter are useful (it can be improved to be 1/2 if the proportion of the samples exploited by the two parties to analyze the security of the quantum channel to all the instances obtained is small). As the symmetry of the encoding states shown in Eqs. (19)–(22), we get a scheme quite similar to a BB84 QKD protocol [1] with four-dimensional quantum systems. However, the scheme introduced in Ref. [23] is more similar to the B92 QKD protocol [2]. Through a channel with loss, our QKD scheme may be more secure than that in Ref. [23].

The idea of using only a few X bases to check the eavesdropping was proposed ten years ago [29]. Its main aim is to reduce the fraction of discarded data caused by wrong basis measurement. There are some differences between it and our schemes. First, in Ref. [29] a predominant basis is used to prepare and measure the states, but in ours a predominant basis is only used to distill the key bits. That is, states transmitting in the quantum channel are completely random in the four states in our schemes, so that a refined analysis of error rate was required to prevent the eavesdropper from getting information using the predominant basis in the former, while the error rate analysis of ours is similar to the BB84 QKD protocol, as is the security. Second, the samples for the eavesdropping check are chosen by Bob, which makes the process efficient as each one selected is useful.

In summary, we propose two QKD schemes to share a sequence of key with two different kinds of collective-noise channels. The interference and two-way quantum communication are not required to solve the problem of collective noises. Despite a little difference in measuring bases and the states used to encode the logical bits, the essence of these two schemes is quite similar. That is, the legitimate user utilizes the special Bell states which are invariant under the given noise model to protect the system against the noise and introduces the spatial degree of freedom to form two nonorthogonal bases with which the key rate is increased compared to protocols abandoning half instances due to wrong measuring bases. There are several remarkable advantages in our two schemes. First, the samples for the security check are not asked to be measured with an entangled basis. The samples are chosen randomly by the receiver Bob, which is easier, compared with the QKD schemes with a decoy state, in which the sender Alice inserts her decoy state into the massage sequence and tells Bob the positions after the transmission. Second, it is unnecessary for the two parties to discard samples. Except for the eavesdropping check, almost all of the states transmitted are used to share the private key. Moreover, although the logical bits are encoded into entangled states, the receiver only needs to perform single-particle product measurements on his photons, not joint two-particle Bell-state measurements. Except for the requirement of two nonorthogonal bases measurement for the eavesdropping check, Bob need not switch his two conjugate bases to obtain the key. Only passive detection is enough to get the message.

Schemes using several physical bits to present one logical bit are fragile with photon loss and hence the communication distance is restricted. This is a tradeoff between the transmission distance and the degree of fault tolerance. More research and development of technique are expected to solve this problem in the future.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China under Grant No. 10604008, a Foundation for the Author of National Excellent Doctoral Dissertation of China under Grant No. 200723, and Beijing Natural Science Foundation under Grant No. 1082008.

[1] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[2] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[6] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).
[7] F. G. Deng and G. L. Long, Phys. Rev. A **68**, 042315 (2003).
[8] F. G. Deng and G. L. Long, Phys. Rev. A **70**, 012311 (2004).
[9] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[10] H. K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
[11] C. Kurtsiefer, P. Zarda, and M. Halder, Nature (London) **419**, 450 (2002).
[12] D. Stucki, N. Ginsin, O. Guinnard, and H. Zbinden, New J. Phys. **4**, 41 (2002).
[13] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Gan, Opt. Lett. **30**, 2632 (2005).
[14] M. Martinelli, Opt. Commun. **72**, 341 (1989).
[15] F. G. Deng, X. H. Li, H. Y. Zhou, and Z. J. Zhang, Phys. Rev. A **72**, 044302 (2005); X. H. Li, F. G. Deng, and H. Y. Zhou, *ibid.* **74**, 054302 (2006).
[16] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[17] D. Kalamidas, Phys. Lett. A **343**, 331 (2005).
[18] X. H. Li, F. G. Deng, and H. Y. Zhou, Appl. Phys. Lett. **91**, 144101 (2007).
[19] X. B. Wang, Phys. Rev. Lett. **92**, 077902 (2004).
[20] X. B. Wang, Phys. Rev. A **69**, 022320 (2004).
[21] Y. A. Chen, A. N. Zhang, Z. Zhao, X. Q. Zhou, and J. W. Pan, Phys. Rev. Lett. **96**, 220504 (2006).
[22] Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. Lett. **91**, 087901 (2003).
[23] J. C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. **92**, 017901 (2004).
[24] X. B. Wang, Phys. Rev. A **72**, 050304(R) (2005).
[25] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[26] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[27] J. W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **86**, 4435 (2001).
[28] C. Simon and J. W. Pan, Phys. Rev. Lett. **89**, 257901 (2002).
[29] M. Ardehali, H. F. Chau, and Hoi-Kwong Lo, e-print arXiv:quant-ph/9803007.
[30] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).