Quantum key distribution with entangled photon sources

Xiongfeng Ma,* Chi-Hang Fred Fung,† and Hoi-Kwong Lo‡
Center for Quantum Information and Quantum Control, Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario, Canada M5S 1A7
(Received 5 April 2007; published 11 July 2007)

A parametric down-conversion (PDC) source can be used as either a triggered single-photon source or an entangled-photon source in quantum key distribution (QKD). The triggering PDC QKD has already been studied in the literature. On the other hand, a model and a post-processing protocol for the entanglement PDC QKD are still missing. We fill in this important gap by proposing such a model and a post-processing protocol for the entanglement PDC QKD. Although the PDC model is proposed to study the entanglement-based QKD, we emphasize that our generic model may also be useful for other non-QKD experiments involving a PDC source. Since an entangled PDC source is a basis-independent source, we apply Koashi and Preskill's security analysis to the entanglement PDC QKD. We also investigate the entanglement PDC QKD with two-way classical communications. We find that the recurrence scheme increases the key rate and the Gottesman-Lo protocol helps tolerate higher channel losses. By simulating a recent 144-km open-air PDC experiment, we compare three implementations: entanglement PDC QKD, triggering PDC QKD, and coherent-state QKD. The simulation result suggests that the entanglement PDC QKD can tolerate higher channel losses than the coherent-state QKD. The coherent-state QKD with decoy states is able to achieve highest key rate in the low- and medium-loss regions. By applying the Gottesman-Lo two-way post-processing protocol, the entanglement PDC QKD can tolerate up to 70 dB combined channel losses (35 dB for each channel) provided that the PDC source is placed in between Alice and Bob. After considering statistical fluctuations, the PDC setup can tolerate up to 53 dB channel losses.

DOI: 10.1103/PhysRevA.76.012307 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

There are mainly two types of quantum key distribution (QKD) schemes. One is the prepare-and-measure scheme such as the Bennett-Brassand (BB84) 1984 protocol [1], and the other is the entanglement-based QKD such as the Ekert 1991 (Ekert91) protocol [2] and Bennett-Brassard-Mermin 1992 (BBM92) [3] protocol. The security of both types of QKD has been proven in the last decade; see, for example, [4–6]. For a review of quantum cryptography, one may refer to [7]. Meanwhile, researchers have also proven the security of the QKD with realistic devices, such as [8–14].

In the original proposal of the BB84 protocol, a single-photon source is required. Unfortunately, single-photon sources are still not commercially available. Instead, a weak coherent-state source is widely used as an imperfect single-photon source. Throughout this paper, we call this implementation the coherent-state QKD. Many coherent-state QKD experiments have been performed since the first QKD experiment [15]; see, for example, [16–21].

The decoy-state method [22] has been proposed as a useful method for substantially improving the performance of the coherent-state QKD. The security of the QKD with decoy states has been proven [23–25]. Asymptotically, the coherent-state QKD with decoy states is able to operate as good as a QKD with perfect single-photon sources in the sense that the key generation rates given by both setups linearly depend on the channel transmittance [25]. Afterwards, some practical decoy-state protocols are proposed [26–29]. Experimental demonstrations of the decoy-state method have been done recently [30–35]. Other than the decoy-state method, there are other approaches to enhance the performance of the coherent-state QKD, such as a QKD with strong reference pulses [36,37] and differential-phase-shift QKD [38].

Besides the coherent source, there is another source that can be used for the QKD: parametric down-conversion (PDC) source. With a PDC source, one can realize either prepare-and-measure or entanglement-based QKD protocols [39]. To implement a prepare-and-measure QKD protocol, one can use a PDC source as a triggered single-photon source. To implement an entanglement-based QKD protocol, on the other hand, one can use the polarization entanglement between two modes of the light emitted from a PDC source. We call these two implementations triggering PDC QKD and entanglement PDC QKD. With an entangled source, one can also implement QKD protocols based on causality [40] and Bell's inequality [41]. We notice that the PDC QKD based on time-energy entanglement has been exploited [42].

The model and post-processing of the triggering PDC QKD have already been studied [9]. Recently, there have been some practical decoy-state proposals for the triggering PDC QKD [43–45]. In this paper, we will focus on the asymptotic decoy-state protocol [25], which is the upper bound of all these practical decoy-state protocols when threshold detectors are used by Alice and Bob.

On the other hand, the model and post-processing for the entanglement PDC QKD are still missing. In this paper, we present a model for the entanglement PDC QKD. From the model, we find that an entangled PDC source is a basis-

*xima@physics.utoronto.ca
†cffung@comm.utoronto.ca
‡hklo@comm.utoronto.ca

independent source for the QKD. Based on this observation, we propose a post-processing scheme by applying Koashi and Preskill's security analysis [13].

Recently, a free-space distribution of entangled photons over 144 km has been demonstrated [46]. We simulate this experiment setup and compare three QKD implementations: entanglement PDC QKD, triggering PDC QKD, and coherent-state QKD. In the simulation, we also apply the Gottesman-Lo two-way post-processing protocol [47] and a recurrence scheme [48]; see also [49].

The main contributions of this paper are the following.

(i) We present a model for the entanglement PDC QKD. Although the model is proposed to study the entanglement-based QKD, this generic model may also be useful for other non-QKD experiments involving a PDC source.

(ii) From the model, we find that an entangled PDC source is a basis-independent source for QKD. Based on this observation, we propose a post-processing scheme for the entanglement PDC QKD. Essentially, we apply Koashi and Preskill's security analysis [13].

(iii) By simulating a PDC experiment [46], we compare three QKD implementations: entanglement PDC QKD, triggering PDC QKD, and coherent-state QKD. In the entanglement PDC QKD, we consider two cases: source in the middle and source on Alice's side.

(iv) In the case that the PDC source is placed in between Alice and Bob, we find that the entanglement PDC QKD can tolerate the highest channel losses, up to 70 dB, by applying Gottesman-Lo two-way classical communication post-processing protocol [47]. We remark that a 35-dB channel loss is comparable to the estimated loss in a satellite-to-ground transmission in the literature [50–54].

(v) We consider statistical fluctuations for the entanglement PDC QKD. In this case, the PDC setup can tolerate up to 53 dB channel loss.

(vi) The coherent state QKD with decoy states is able to achieve highest key rate in the low- and medium-loss regions.

In Sec. II, we will review two experiment setups of the entanglement PDC QKD. In Sec. III, we will model the entanglement PDC QKD. In Sec. IV, we will propose a post-processing scheme for the entanglement PDC QKD. In Sec. V, we will compare the entanglement PDC QKD, the triggering PDC QKD, and the coherent-state QKD by simulating a real PDC experiment. We also apply protocols based on two-way classical communications and consider statistical fluctuations. In Appendix A, we calculate the quantum bit error rate in the entanglement PDC QKD. In Appendix B, we investigate the optimal μ for the entanglement PDC QKD.

II. IMPLEMENTATION

In general, the PDC source does not necessarily belong to one of the two legitimate users of QKD, Alice or Bob. One can even assume that an eavesdropper, Eve, owns the PDC source. In this section we will compare two experimental setups of the entanglement PDC QKD due to the position of the PDC source, in between Alice and Bob or on Alice's side.

Let us start with a general discussion about an entangled PDC source. With the rotating-wave approximation, the Hamiltonian of the PDC process can be written as [55]

$$H = i\chi(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger) + \text{H.c.}, \tag{1}$$

where "H.c." means Hermitian conjugate and χ is a coupling constant depending on the crystal nonlinearity and the amplitude of the pump beam. The operators a_i and b_i are the annihilation operators for rectilinear polarizations $i \in \{H, V\}$ in mode a and mode b, respectively. Mode a and mode b are the modes sent to Alice and Bob, respectively.

In Sec. III, we will focus on modeling the measurement of the rectilinear polarization (Z) basis. Due to symmetry, all the calculations can be applied to the X basis too.

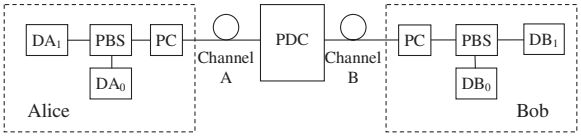

FIG. 1. A schematic diagram for the entanglement PDC QKD. Alice and Bob connect to a entangled PDC source by optical links. They each receive one of two entangled modes coming out from the PDC source. Both Alice and Bob randomly choose the basis (by polarization controllers) to measure the arrived signals (by single-photon detectors). PC: polarization controller. PBS: polarized beam splitter. DA_0, DA_1, DB_0, DB_1: threshold detectors.

A. Source in the middle

First we consider the case that the PDC source sits in between Alice and Bob. The schematic diagram is shown in Fig. 1.

As shown in Fig. 1, a PDC source provides two entangled modes a and b, which are sent to Alice and Bob, respectively. After receiving the signals, Alice and Bob each randomly choose a basis (X or Z) to perform a measurement. One key observation of this setup is that the state emitted from the PDC source is independent of the bases Alice and Bob choose for the measurements.

B. Source on Alice's side

Another case is that Alice owns the PDC source. The schematic diagram is shown in Fig. 2.

Comparing Figs. 1 and 2, we can see that the only difference is the position of the PDC source. As we will see in Sec. IV, the post-processings of these two setups are similar.

We remark that in the second setup, Alice's measurement commutes with Bob's measurement. Thus, we have the same observation as before: that the PDC source state is independent of the measurement bases.

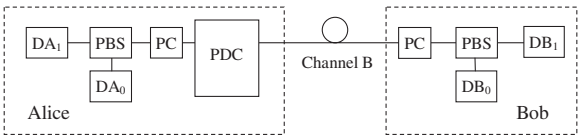

FIG. 2. A schematic diagram for the entanglement PDC QKD. Alice measures one of the entangled modes coming out from the PDC source and sends Bob the other mode.

Therefore, for both setups the entangled PDC source is a basis-independent source. It follows that the entanglement PDC QKD is a basis-independent QKD.

III. MODEL

In this section, we will model entangled PDC sources, channel, and detectors for the entanglement PDC QKD. We emphasize that this model is applicable for both experiment setups described in Sec. II.

A. Entangled PDC source

From Eq. (1), the state emitted from a type-II PDC source can be written as [55]

$$|\Psi\rangle = (\cosh\chi)^{-2}\sum_{n=0}^{\infty}\sqrt{n+1}\tanh^{n}\chi|\Phi_n\rangle, \tag{2}$$

where $|\Phi_n\rangle$ is the state of an n-photon pair, given by

$$|\Phi_n\rangle = \frac{1}{\sqrt{n+1}}\sum_{m=0}^{n}(-1)^m|n-m,m\rangle_a|m,n-m\rangle_b. \tag{3}$$

For example, when $n=1$, Eq. (3) will give a Bell state

$$|\Phi_1\rangle = \frac{1}{\sqrt{2}}(|1,0\rangle_a|0,1\rangle_b - |0,1\rangle_a|1,0\rangle_b)$$
$$= \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle_a|\updownarrow\rangle_b - |\updownarrow\rangle_a|\leftrightarrow\rangle_b). \tag{4}$$

Here we use the polarizations $|1,0\rangle=|\leftrightarrow\rangle$ and $|0,1\rangle=|\updownarrow\rangle$ as a qubit basis (Z basis) for QKD. From Eq. (2), the probability to get an n-photon pair is

$$P(n) = \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}, \tag{5}$$

where we define $\lambda \equiv \sinh^2\chi$. The expected photon pair number is $\mu=2\lambda$, which is the average number of photon pairs generated by one pump pulse, characterizing the brightness of a PDC source.

B. Detection

We assume that the detection probabilities of the photons in the state of Eq. (3) are independent. Define η_A and η_B to be the detection efficiencies for Alice and Bob, respectively. Both η_A and η_B take into account the channel losses, detector efficiencies, coupling efficiencies, and losses inside the detector box. For an n-photon pair, the overall transmittance is

$$\eta_n = [1-(1-\eta_A)^n][1-(1-\eta_B)^n]. \tag{6}$$

We remark that the channel loss is included in η_A and η_B. Thus, this model can be applied to either of following two cases: (a) the PDC source is in between Alice and Bob or (b) the PDC source is on Alice (or Bob)'s side.

Yield. Define Y_n to be the yield of an n-photon pair—i.e., the conditional probability of a coincidence detection event given that the PDC source emits an n-photon pair. Y_n mainly comes from two parts: the background and the true signal. Assuming that the background counts are independent of the signal photon detection, then Y_n is given by

$$Y_n = [1-(1-Y_{0A})(1-\eta_A)^n][1-(1-Y_{0B})(1-\eta_B)^n], \tag{7}$$

where Y_{0A} and Y_{0B} are the background count rates on Alice's and Bob's sides, respectively. The vacuum-state contribution is $Y_0=Y_{0A}Y_{0B}$. The *gain* of the n-photon pair Q_n, which is the product of Eqs. (5) and (7), is given by

$$Q_n = Y_nP(n) = [1-(1-Y_{0A})(1-\eta_A)^n]$$
$$\times[1-(1-Y_{0B})(1-\eta_B)^n]\frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}. \tag{8}$$

The overall gain is given by

$$Q_\lambda = \sum_{n=0}^{\infty}Q_n = 1-\frac{1-Y_{0A}}{(1+\eta_A\lambda)^2}-\frac{1-Y_{0B}}{(1+\eta_B\lambda)^2}$$
$$+\frac{(1-Y_{0A})(1-Y_{0B})}{(1+\eta_A\lambda+\eta_B\lambda-\eta_A\eta_B\lambda)^2}. \tag{9}$$

Here the overall gain Q_λ is the probability of a coincident detection event given a pump pulse. Note that the parameter λ is one-half of the expected photon pair number μ.

The overall quantum bit error rate (QBER, E_λ) is given by

$$E_\lambda Q_\lambda = e_0Q_\lambda - \frac{2(e_0-e_d)\eta_A\eta_B\lambda(1+\lambda)}{(1+\eta_A\lambda)(1+\eta_B\lambda)(1+\eta_A\lambda+\eta_B\lambda-\eta_A\eta_B\lambda)}, \tag{10}$$

where Q_λ is the gain given in Eq. (9). The calculation of the E_λ is shown in Appendix A.

IV. POST-PROCESSING

As mentioned in Sec. II, the entanglement PDC QKD is a basis-independent QKD. Thus, we can apply Koashi and Preskill's security proof [13]. The key generation rate is given by

$$R \geq q\{Q_\lambda[1-f(\delta_b)H_2(\delta_b)-H_2(\delta_p)]\}, \tag{11}$$

where q is the basis reconciliation factor (1/2 for the BB84 protocol due to the fact that half of the time Alice and Bob disagree with the bases, and if one uses the efficient BB84 protocol [56], $q\approx 1$), the subscript λ denotes one-half of the expected photon number μ, Q_λ is the overall gain, δ_b (δ_p) is the bit (phase) error rate, $f(x)$ is the bidirection error correction efficiency (see, for example, [57]) as a function of error rate, normally $f(x)\geq 1$ with Shannon limit $f(x)=1$, and $H_2(x)$ is the binary entropy function,

$$H_2(x) = -x\log_2(x)-(1-x)\log_2(1-x).$$

Due to the symmetry of X- and Z-basis measurements, as shown in Sec. II, δ_b and δ_p are given by

$$\delta_b = \delta_p = E_\lambda, \tag{12}$$

where E_λ is the overall QBER. This equation is true for the asymptotic limit of an infinitely long key distribution. Later

TABLE I. Experimental parameters deduced from the 144-km PDC experiment [46]. Here we assume that Alice and Bob use detectors with the same characteristics. e_d is the intrinsic detector error rate. Y_0 is the background count rate. η_{Alice} (η_{Bob}) is the detection efficiency in Alice's (Bob's) box, including detector efficiency and internal optical losses. The overall transmittance η_A (η_B) is the product of Alice's (Bob's) channel transmission efficiency and η_{Alice} (η_{Bob}).

Repetition rate	Wavelength	η_{Alice}	η_{Bob}	e_d	Y_0
249 MHz	710 nm	14.5%	14.5%	1.5%	6.02×10^{-6}

in Sec. V C, we will see that Eq. (12) may not be true when statistical fluctuations are taken into account.

We remark that in Koashi and Preskill's security proof, the squash model [14] is applied. In the squash model, Alice and Bob project the state onto the qubit Hilbert space before X or Z measurements. For more details of the squash model, one can refer to [14]. In the case that Alice owns the PDC source, as discussed in Sec. II B, the key rate formula of Eq. (11) has been proven [58] to be valid for the QKD with threshold detectors without the squash model; see also [59]. We also notice that this post-processing scheme, Eqs. (11) and (12), can also be derived from a security analysis based on the uncertainty principle [60].

In Eq. (11), Q_λ can be directly measured from a QKD experiment and E_λ can be estimated by error testing. In the simulation shown in Sec. V, we will use Eqs. (9) and (10).

We remark that the post-processing for the entanglement PDC QKD is simpler than the coherent-state QKD and triggering PDC QKD. In the entanglement PDC QKD, all the parameters needed for the post-processing (Q_λ and E_λ) can be directly calculated or tested from the measured classical data. In the coherent PDC QKD and the triggering PDC QKD, on the other hand, Alice and Bob need to know the value of some experimental parameters ahead, such as the expected photon number μ, and also need to estimate the gain and error rate of the single-photon states Q_1 and e_1, which make the statistical fluctuation analysis difficult [29].

The post-processing can be further improved by introducing two-way classical communications between Alice and Bob [47,49]. Also, the adding noise technique may enhance the performance [61].

V. SIMULATION

In this section, we will first compare three QKD implementations: entanglement PDC QKD, triggering PDC QKD, and coherent-state QKD. Then we will apply post-processing protocols with two-way classical communications to the entanglement PDC QKD. Finally, we will consider statistical fluctuations.

We deduce experimental parameters from Ref. [46] due to the model given in Sec. III, which are listed in Table I. For the coherent-state QKD, we use $\eta_A=1$ since Alice prepares the states in this case. In the following simulations, we will use $q=1/2$ and $f(E_\mu)=1.22$ [57].

The optimal expected photon number μ of the coherent-state QKD has been discussed in Refs. [9,29]. In Appendix B, we investigate the optimal μ (2λ) for the entanglement PDC QKD. Not surprisingly, we find that the optimal μ for the entanglement PDC QKD is on the order of 1, $\mu=2\lambda=O(1)$. Thus, the key generation rate given in Eq. (11) depends linearly on the channel transmittance.

A. Comparison of three QKD implementations

In the first simulation, we assume that Alice is able to adjust the expected photon pair number μ (2λ, the brightness of the PDC source) in the region of $[0,1]$. Thus, we can optimize μ for the entanglement PDC QKD and the triggering PDC QKD. The simulation results are shown in Fig. 3.

From Fig. 3, we have the following remarks.

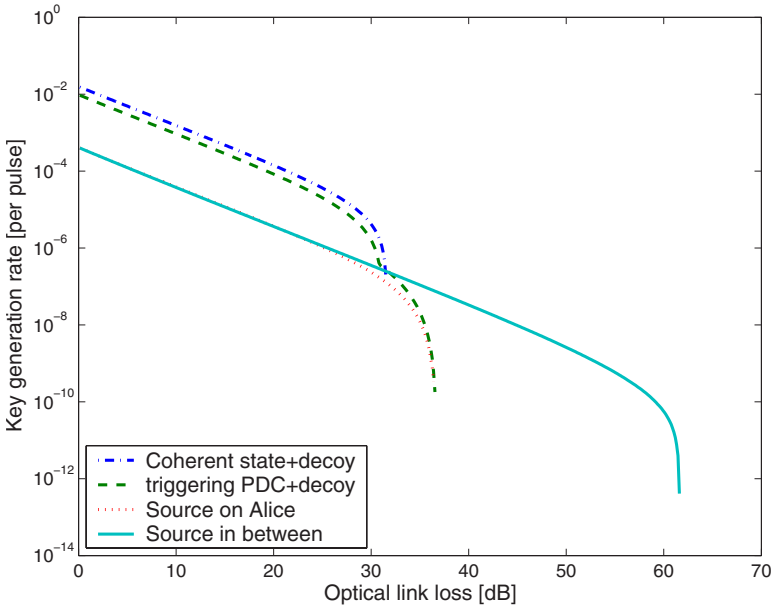

FIG. 3. (Color online) Plot of the key generation rate in terms of the optical loss, comparing four cases: coherent-state QKD+aysmptotic decoy, triggering PDC+asymptotic decoy, and entanglement PDC QKD (source in the middle and source on Alice's side). For the coherent state QKD+decoy, we use $\eta_A=1$. We numerically optimize μ (2λ) for each curve.

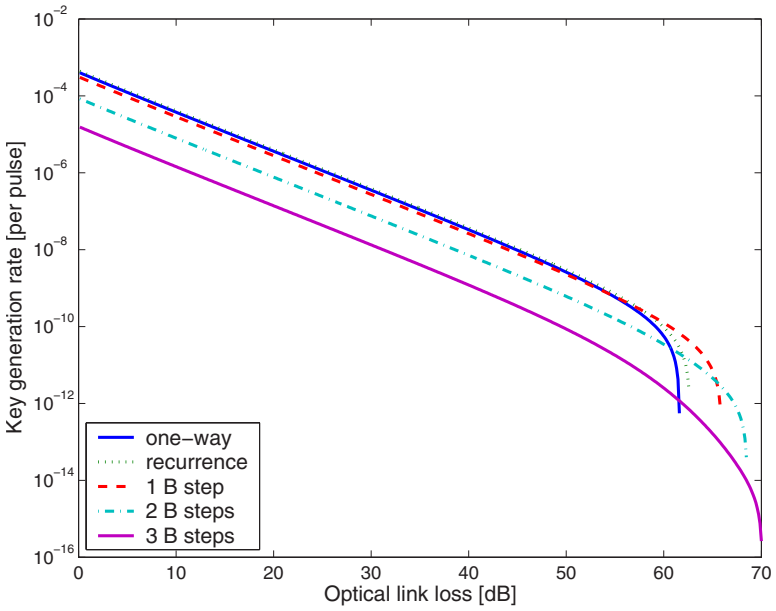

FIG. 4. (Color online) Plot of the key generation rate in terms of the optical loss. We apply the recurrence idea and up to 3 B steps. μ is numerically optimized for each curve.

(i) The entanglement PDC QKD can tolerate the highest channel losses in the case that the source is placed in the middle between Alice and Bob.

(ii) The coherent-state QKD with decoy states is able to achieve the highest key rate in the low- and medium-loss regions. This is because in the coherent-state QKD implementation, Alice does not need to detect any photons, which will effectively give $\eta_A=1$ in the PDC QKD implementations.

(iii) Comparing two cases of the entanglement PDC QKD—source in the middle and source on Alice's side—they yield similar key rates in the low and medium regions. But the source in the middle case can tolerate higher channel losses.

In the following simulations, we will focus on the case that the entangled PDC source sits in the middle between Alice and Bob.

B. With two-way classical communications

We can also apply the idea of post-processing with two-way classical communications. Similar to the argument of Ref. [49], we combine the recurrence idea [48] and the B steps in the Gottesman-Lo protocol [47]. The simulation results are shown in Fig. 4.

From Fig. 4, we can see that the recurrence scheme can increase the key rate by around 10% and extend the maximal tolerable loss by around 1 dB. The PDC experiment setup can tolerate up to 70 dB channel loss with 3 B steps. We remark that 70 dB (35 dB in each channel) is comparable to the estimated loss in a satellite-to-ground transmission [53]. This result suggests that a satellite-ground QKD may be possible. However, this simulation assumes the ideal situation that an infinite number of signals are transmitted. Moreover, we assume that μ (the brightness of the PDC source) is a freely adjustable parameter in the PDC experiment. In a more realistic case where a finite number of signals are transmitted and μ is a fixed parameter, the tolerable channel loss becomes smaller, as we show next.

C. Statistical fluctuations

In Eq. (12), we assume that δ_b and δ_p are the same due to the symmetry between X and Z measurements. Alice and Bob randomly choose to measure in the X or Z basis. Then, asymptotically, δ_b is a good estimate of δ_p. However, in a realistic QKD experiment, only a finite number of signals are transmitted. Thus δ_p may slightly differ from δ_b. We assume that Alice and Bob do not perform error testing explicitly. Instead, they obtain the bit error rate directly from an error correction protocol (e.g., the cascade protocol [57]). In that case, there is no fluctuation in the bit error rate $\delta_b=E_\lambda$. On the other hand, the phase error rate may fluctuate to some certain value $\delta_p=\delta_b+\epsilon$. Following the fluctuation analysis of Ref. [6], we know that the probability to get a ϵ bias is

$$P_\epsilon \leq \exp\left(-\frac{\epsilon^2 n}{4\delta_b(1-\delta_b)}\right), \tag{13}$$

where $n=NQ_\lambda$ the number of detection events, the product of total number of pulses N, and the overall gain Q_λ.

In the 144-km PDC experiment [46], the repetition rate of pump pulse is 249 MHz, as given in Table I. As discussed in Ref. [53], the typical time of ground-satellite QKD allowed by satellite visibility is 40 min. Here, we assume the experiment runs 10 min, which means that the data size is $N=1.5\times10^{11}$. By taking this data size, we consider the fluctuations for the entanglement PDC QKD.

In the realistic case, the brightness of the PDC source μ cannot be set freely. In the 144-km PDC experiment [46], the expected photon pair number is $\mu=2\lambda=0.053$. After taking $\mu=0.053$ and a data size of $N=1.5\times10^{11}$ for the fluctuation analysis, the simulation result is shown in Fig. 5.

We have a couple remarks on Fig. 5.

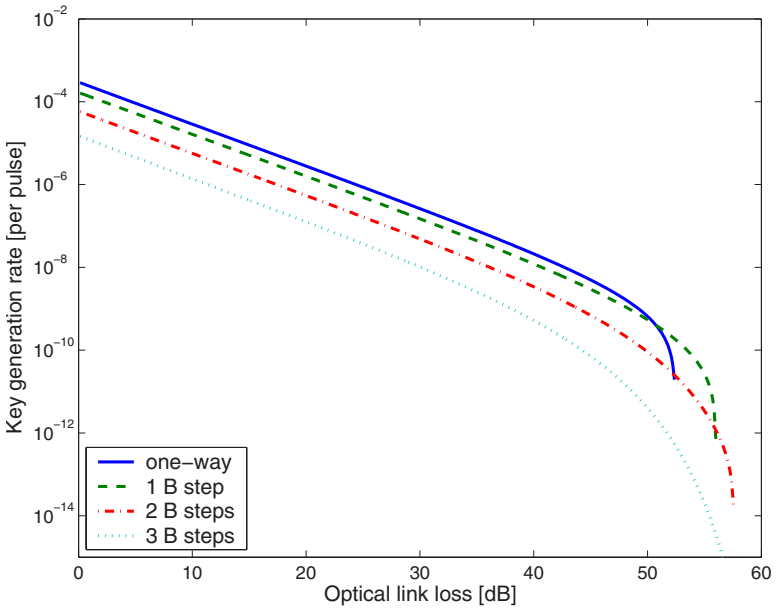

FIG. 5. (Color online) Plot of the key generation rate in terms of the optical loss. We take a realistic $\mu=2\lambda=0.053$ and consider the fluctuation with a data size of $N=1.5\times10^{11}$ and a confident interval of $1-P_{\epsilon}\geq1-e^{-50}$.

(i) In Fig. 5, if we cut off from the key rate of 10^{-10},[1] the entanglement PDC QKD with one B step can tolerate up to 53 dB transmission loss.

(ii) We have tried simulations with various μ's. We find that the key rate is stable with moderate changes of μ. With the above fluctuation analysis, if we numerically optimize μ for each curve, the maximal tolerable channel loss (with a cutoff key rate of 10^{-10}) is only 1 dB larger than the one given by $\mu=0.053$. Thus, one cannot significantly improve the maximal tolerable channel loss by just using a better PDC source in the 144-km PDC experiment setup [46].

VI. CONCLUSION

We have proposed a model and post-processing for the entanglement PDC QKD. We find that the post-processing is simple by applying Koashi and Preskill's security proof due to the fact that the entanglement PDC QKD is a basis-independent QKD. Specifically, only directly measured data (the overall gain and the overall QBER) are needed to perform the post-processing. By simulating a recent experiment, we compare three QKD schemes: coherent-state QKD +aysmptotic decoy, triggering PDC+asymptotic decoy, and entanglement PDC QKD (source in the middle and on Alice's side). We find that (a) the entanglement PDC (with source in the middle) can tolerate the highest channel loss; (b) the coherent-state QKD with decoy states can achieve the highest key rate in the medium- and low-loss regions; (c) asymptotically, with a realistic PDC experiment setup, the entanglement PDC QKD can tolerate up to 70 dB channel losses by applying post-processing schemes with two-way classical communications; (d) the PDC setup can tolerate up to 53 dB channel losses when statistical fluctuations are taken into account.

[1]Then the final key length is 15 bits. One should also consider the cost in the authentication procedure. Thus, this is a reasonable cutoff point.

ACKNOWLEDGMENTS

We thank R. Adamson, C. Erven, A. M. Steinberg, and G. Weihs for enlightening discussions. This work has been supported by CFI, CIAR, CIPI, Connaught, CRC, MITACS, NSERC, OIT, PREA, and the University of Toronto. This research is supported by the Perimeter Institute for Theoretical Physics. Research at the Perimeter Institute is supported in part by the Government of Canada through NSERC and by the province of Ontario through MEDT. X.M. gratefully acknowledges a Chinese Government Award for Outstanding Self-financed Students Abroad. C.-H.F.F. gratefully acknowledges the Walter C. Sumner Memorial and the Shahid U.H. Qureshi Memorial for support.

APPENDIX A: QUANTUM BIT ERROR RATE

Here we will study the quantum bit error rate of the entanglement PDC QKD. Our objective is to derive the QBER formula given in Eq. (10) used in the simulation. The QBER has three main contributions: (i) background counts, which are random noises $e_0=1/2$; (ii) intrinsic detector error e_d, which is the probability that a photon will hit the erroneous detector and characterizes the alignment and stability of the optical system between Alice's and Bob's detection systems; (iii) errors introduced by multiphoton-pair states: (a) Alice and Bob may detect different photon pairs and (b) double clicks. Due to the strong pulsing attack [62], we assume that Alice and Bob will assign a random bit when they get a double click. In either case, the error rate will be $e_0=1/2$.

Let us start with the single-photon-pair case, a Bell state given in Eq. (4). The error rate of single-photon pair e_1 has two sources: background counts and intrinsic detector errors,

$$e_1=e_0-\frac{(e_0-e_d)\eta_A\eta_B}{Y_1}. \tag{A1}$$

If we neglect the case that both background and true signal cause clicks, then e_1 can be written as

$$e_1 \approx \frac{e_0(Y_{0A}Y_{0B} + Y_{0A}\eta_B + \eta_A Y_{0B}) + e_d\eta_A\eta_B}{Y_1}, \quad \text{(A2)}$$

where $e_0=1/2$ is the error rate of background counts. The first term of the numerator is the background contribution and the second term comes from the errors of true signals.

In the following, we will discuss the errors introduced by multiphoton-pair states, e_n, with $n \geq 2$. Here we assume that Alice and Bob use threshold detectors, which can only tell whether the incoming state is a vacuum or nonvacuum. One can imagine the detection of an n-photon-pair state as follows.

(i) Alice and Bob project the n-photon-pair state, Eq. (3), into the $Z^{\otimes n}$ basis.

(ii) Afterwards, they detect each photon with certain probabilities (η_A for Alice and η_B for Bob).

(iii) If either Alice or Bob detects a vacuum, then we regard it as a *loss*. If Alice and Bob both detect a nonvacuum only in one polarization ($\leftrightarrow or \updownarrow$), we regard it as a *single-click* event. Otherwise, we regard it as a *double-click* event.

The state of a two-photon-pair state, according to Eq. (3), can be written as

$$\begin{aligned}|\Phi_2\rangle &= \frac{1}{\sqrt{3}}(|2,0\rangle_a|0,2\rangle_b - |1,1\rangle_a|1,1\rangle_b + |0,2\rangle_a|2,0\rangle_b \\ &= \frac{1}{\sqrt{3}}\Bigg[|\leftrightarrow\ \leftrightarrow\rangle_a|\updownarrow\ \updownarrow\rangle_b - \frac{1}{2}(|\leftrightarrow\ \updownarrow\rangle + |\updownarrow\ \leftrightarrow\rangle)_a \\ &\quad \otimes (|\updownarrow\ \leftrightarrow\rangle + |\leftrightarrow\ \updownarrow\rangle)_b + |\updownarrow\ \updownarrow\rangle_a|\leftrightarrow\ \leftrightarrow\rangle_b\Bigg]. \quad \text{(A3)}\end{aligned}$$

As discussed above, Alice and Bob project the state into the $Z\otimes Z$ basis. If they end up with the first or third state in the brackets of Eq. (A3), they will get perfect anticorrelation, which will not contribute to errors. If they get the second state in the brackets of Eq. (A3), their results are totally independent, which will cause an error with probability $e_0=1/2$. Thus the error probability introduced by a two-photon-pair state is 1/6. Here we have only considered the errors introduced by multiphoton states, item (iii) discussed in the beginning of this Appendix. We should also take into account the effects of background counts and intrinsic detector errors. With these modifications, the error rate of the two-photon-pair state is given by

$$e_2 = e_0 - \frac{2(e_0-e_d)[1-(1-\eta_A)^2][1-(1-\eta_B)^2]}{3Y_2}, \quad \text{(A4)}$$

where Y_2 is given in Eq. (7). Equation (A4) can be understood as follows. Only when Alice and Bob project the Eq. (A3) into $|\leftrightarrow\leftrightarrow\rangle_a|\updownarrow\updownarrow\rangle_b$ or $|\updownarrow\updownarrow\rangle_a|\leftrightarrow\leftrightarrow\rangle_b$ and no background count occurs can they have a probability of e_d to get the wrong answer. Given a coincident detection, the conditional probability for this case is $2[1-(1-\eta_A)^2][1-(1-\eta_B)^2]/3Y_2$. All other cases—a background count, a double click, and measuring different photon pairs—will contribute an error probability $e_0=1/2$.

Next, let us study the errors coming from the state $|n-m,m\rangle_a|m,n-m\rangle_b$. When Alice detects at least one of $n-m$ $|\updownarrow\rangle$ photons but none of m $|\leftrightarrow\rangle$ photons and Bob detects at least one of $n-m$ $|\leftrightarrow\rangle$ photons but none of m $|\updownarrow\rangle$ photons, or both Alice and Bob have bit flips of this case, they will end up with an error probability of e_d. Given a coincident detection, the conditional probability for these two cases is

$$\begin{aligned}&\frac{1}{Y_n}\{[1-(1-\eta_A)^{n-m}](1-\eta_A)^m[1-(1-\eta_B)^{n-m}](1-\eta_B)^m \\ &+[1-(1-\eta_A)^m](1-\eta_A)^{n-m}[1-(1-\eta_B)^m](1-\eta_B)^{n-m}\}.\end{aligned}$$

When Alice detects at least one of $n-m$ $|\updownarrow\rangle$ polarizations but none of m $|\leftrightarrow\rangle$ polarizations and Bob detects at least one of m $|\updownarrow\rangle$ polarizations but none of $n-m$ $|\leftrightarrow\rangle$ polarizations, or both Alice and Bob have bit flips of this case, they will end up with an error probability of $1-e_d$. Given a coincident detection, the conditional probability for these two case is

$$\begin{aligned}&\frac{1}{Y_n}\{[1-(1-\eta_A)^m](1-\eta_A)^{n-m}[1-(1-\eta_B)^{n-m}](1-\eta_B)^m \\ &+[1-(1-\eta_A)^{n-m}](1-\eta_A)^m[1-(1-\eta_B)^m](1-\eta_B)^{n-m}\}.\end{aligned}$$

For all other cases, the error probability is e_0. Thus the error probability for the state $|n-m,m\rangle_a|m,n-m\rangle_b$ is

$$\begin{aligned}e_{nm} &= e_0 - \frac{e_0-e_d}{Y_n}\{(1-\eta_A)^{n-m}(1-\eta_B)^{n-m}[1-(1-\eta_A)^m] \\ &\quad \times[1-(1-\eta_B)^m] + (1-\eta_A)^m(1-\eta_B)^m[1-(1-\eta_A)^{n-m}] \\ &\quad \times[1-(1-\eta_B)^{n-m}] - (1-\eta_A)^{n-m}(1-\eta_B)^m \\ &\quad \times[1-(1-\eta_A)^m][1-(1-\eta_B)^{n-m}] - (1-\eta_A)^m \\ &\quad \times(1-\eta_B)^{n-m}[1-(1-\eta_A)^{n-m}][1-(1-\eta_B)^m]\} \\ &= e_0 - \frac{e_0-e_d}{Y_n}[(1-\eta_A)^{n-m} - (1-\eta_A)^m][(1-\eta_B)^{n-m} \\ &\quad - (1-\eta_B)^m]. \quad \text{(A5)}\end{aligned}$$

In general, for an n-photon-pair state described by Eq. (3), the error rate is given by

$$\begin{aligned}e_n &= \frac{1}{n+1}\sum_{m=0}^{n} e_{nm} = \frac{1}{n+1}\sum_{m=0}^{n} e_0 - \frac{e_0-e_d}{Y_n}[(1-\eta_A)^{n-m} \\ &\quad - (1-\eta_A)^m][(1-\eta_B)^{n-m} - (1-\eta_B)^m] \\ &= e_0 - \frac{e_0-e_d}{(n+1)Y_n}\sum_{m=0}^{n}[(1-\eta_A)^{n-m} - (1-\eta_A)^m][(1-\eta_B)^{n-m} \\ &\quad - (1-\eta_B)^m] \\ &= e_0 - \frac{2(e_0-e_d)}{(n+1)Y_n}\Bigg[\frac{1-(1-\eta_A)^{n+1}(1-\eta_B)^{n+1}}{1-(1-\eta_A)(1-\eta_B)} \\ &\quad - \frac{(1-\eta_A)^{n+1}-(1-\eta_B)^{n+1}}{\eta_B-\eta_A}\Bigg]. \quad \text{(A6)}\end{aligned}$$

The overall QBER is given by

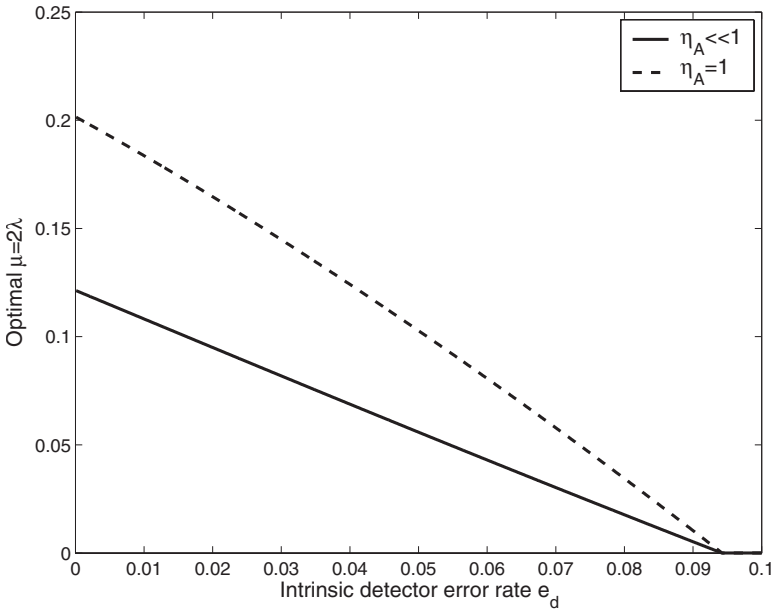

FIG. 6. Plot of the optimal μ in terms of e_d for the entanglement PDC QKD. $f(e_d)=1.22$.

$$E_\lambda Q_\lambda = \sum_{n=0}^{\infty} e_n Y_n P(n)$$
$$= e_0 Q_\lambda - \sum_{n=0}^{\infty} \frac{2(e_0-e_d)\lambda^n}{(1+\lambda)^{n+2}} \left(\frac{1-(1-\eta_A)^{n+1}(1-\eta_B)^{n+1}}{1-(1-\eta_A)(1-\eta_B)} - \frac{(1-\eta_A)^{n+1}-(1-\eta_B)^{n+1}}{\eta_B-\eta_A} \right)$$
$$= e_0 Q_\lambda - \frac{2(e_0-e_d)\eta_A\eta_B\lambda(1+\lambda)}{(1+\eta_A\lambda)(1+\eta_B\lambda)(1+\eta_A\lambda+\eta_B\lambda-\eta_A\eta_B\lambda)}, \quad \text{(A7)}$$

where Q_λ is the gain given in Eq. (9).

APPENDIX B: OPTIMAL μ

The optimal μ for the coherent-state QKD has already been discussed [9,29]. Here we need to find out the optimal μ for the entanglement PDC QKD. In the following calculation, we will focus on optimizing the parameter λ $(=\mu/2)$ for the key generation rate given in Eq. (11).

By assuming η_B to be small and neglecting Y_0, we can simplify Eq. (9):

$$Q_\lambda \approx 2\eta_B\lambda\left(1-\frac{1-\eta_A}{(1+\eta_A\lambda)^3}\right). \quad \text{(B1)}$$

The overall QBER given in Eq. (10) can be simplified to

$$E_\lambda \approx \frac{1}{2} - \frac{(1-2e_d)(1+\lambda)(1+\eta_A\lambda)}{2(1+3\lambda+3\eta_A\lambda^2+\eta_A^2\lambda^3)}. \quad \text{(B2)}$$

In order to maximize the key generation rate, given by Eq. (11), the optimal λ satisfies

$$\frac{\partial Q_\lambda}{\partial\lambda}\{1-[1+f(E_\lambda)]H_2(E_\lambda)\} - Q_\lambda[1+f(E_\lambda)]\frac{\partial E_\lambda}{\partial\lambda}\log_2\frac{1-E_\lambda}{E_\lambda} = 0. \quad \text{(B3)}$$

Here we treat $f(E_\lambda)$ as a constant. In the following we will consider two extremes: $\eta_A \approx 1$ and $\eta_A \ll 1$.

When $\eta_A \approx 1$, the overall gain and QBER are given by

$$Q_\lambda \approx 2\eta_B\lambda,$$
$$E_\lambda \approx \frac{2e_d+\lambda}{2+2\lambda}. \quad \text{(B4)}$$

Thus, Eq. (B3) can be simplified to

$$1-[1+f(E_\lambda)]H_2(E_\lambda) - \lambda[1+f(E_\lambda)]\frac{1-2e_d}{2(1+\lambda)^2}\log_2\frac{1-E_\lambda}{E_\lambda} = 0. \quad \text{(B5)}$$

When $\eta_A \ll 1$,

$$Q_\lambda \approx 2\eta_A\eta_B\lambda(1+3\lambda),$$
$$E_\lambda \approx \frac{e_d+\lambda+e_d\lambda}{1+3\lambda}. \quad \text{(B6)}$$

Thus, Eq. (B3) can be simplified to

$$(1+6\lambda)\{1-[1+f(E_\lambda)]H_2(E_\lambda)\} - \lambda[1+f(E_\lambda)]\frac{1-2e_d}{1+3\lambda}\log_2\frac{1-E_\lambda}{E_\lambda} = 0. \quad \text{(B7)}$$

The solutions to Eqs. (B5) and (B7) are shown in Fig. 6.

From Fig. 6, we can see that the optimal $\mu=2\lambda$ for the entanglement PDC is in the order of 1, $\mu=2\lambda=O(1)$, which will lead to a final key generation rate of $R=O(\eta_A\eta_B)$.

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[4] D. Mayers, J. ACM **48**, 351406 (2001).
[5] H.-K. Lo and H.-F. Chau, Science **283**, 2050 (1999).
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[8] D. Mayers and A. Yao, *FOCS, Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE, Computer Society Press, Los Alamitos, 1998), p. 503.
[9] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[10] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[11] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, J. Mod. Opt. **48**, 2009 (2001).
[12] H. Inamori, N. Lütkenhaus, and D. Mayers, e-print arXiv:quant-ph/0107017 (to be published).
[13] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).
[14] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[15] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. A. Smolin, J. Cryptology **5**, 3 (1992).
[16] P. D. Townsend, IEEE Photonics Technol. Lett. **10**, 1048 (1998).
[17] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett. **34**, 2116 (1998).
[18] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, Opt. Express **4**, 383 (1999).
[19] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature (London) **419**, 450 (2002).
[20] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[21] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, Opt. Lett. **30**, 2632 (2005).
[22] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[23] H.-K. Lo, *Proceedings of IEEE ISIT* (IEEE, New York, 2004), p. 137.
[24] X. Ma, e-print arXiv:quant-ph/0503057.
[25] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[26] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[27] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, e-print arXiv:quant-ph/0503002.
[28] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).
[29] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[30] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[31] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, *Proceedings of IEEE ISIT* (IEEE, New York, 2006), pp. 2094–2098.
[32] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).
[33] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007).
[34] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).
[35] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).
[36] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).
[37] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, e-print arXiv:quant-ph/0607082.
[38] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[39] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).
[40] L. Masanes and A. Winter, e-print arXiv:quant-ph/0606049.
[41] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).
[42] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[43] W. Mauerer and C. Silberhorn, e-print arXiv:quant-ph/0609195.
[44] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, e-print arXiv:quant-ph/0610118.
[45] Q. Wang, X.-B. Wang, and G.-C. Guo, Phys. Rev. A **75**, 012312 (2007).
[46] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, e-print arXiv:quant-ph/0607182.
[47] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[48] Karl Gerd H. Vollbrecht and F. Verstraete, Phys. Rev. A **71**, 062325 (2005).
[49] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, Phys. Rev. A **74**, 032330 (2006).
[50] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, IEEE J. Sel. Top. Quantum Electron. **9**, 1541 (2003).
[51] J. G. Rarity, M. Gorman, P. R. Knight, H. Weinfurter, and C. Kurtsiefer, in *Proceedings of SPIE: Quantum Communications and Quantum Imaging*, edited by R. E. Meyers and Y. Shih (SPIE, New York, 2004), Vol. 5161, p. 240.
[52] R. Kaltenbaek, M. Aspelmeyer, T. Jennewein, C. Brukner, A. Zeilinger, M. Pfennigbauer, and W. R. Leeb, in *Proceedings of SPIE: Quantum Communications and Quantum Imaging*, edited by R. E. Meyers and Y. Shih (SPIE, New York, 2004), Vol. 5161, p. 252.
[53] P. Villoresi, F. Tamburini, M. Aspelmeyer, T. Jennewein, R. Ursin, C. Pernechele, G. Bianco, A. Zeilinger, and C. Barbieri, in *Proceedings of SPIE: Quantum Communications and Quantum Imaging II*, edited by R. E. Meyers and Y. Shih (SPIE, New York, 2004), Vol. 5551, p. 113.
[54] N. Antonietti, M. Mondin, G. Brida, and M. Genovese, Int. J. Quantum Inf. **5**, 241 (2007).
[55] P. Kok and S. L. Braunstein, Phys. Rev. A **61**, 042304 (2000).
[56] H.-K. Lo, H.-F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
[57] G. Brassard and L. Salvail, in *Advances in Cryptology EURO-*

CRYPT '93, edited by G. GoosJ. Hartmanis (Springer-Verlag, Berlin, 1993).
[58] M. Koashi, e-print arXiv:quant-ph/0609180.
[59] H.-K. Lo and J. Preskill, e-print arXiv:quant-ph/0610203.
[60] M. Koashi, J. Phys.: Conf. Ser. **36**, 98 (2006).
[61] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[62] N. Lütkenhaus, Appl. Phys. B: Lasers Opt. **69**, 395 (1999).