Performance of various quantum-key-distribution systems using 1.55-μm up-conversion single-photon detectors

Eleni Diamanti,[1,*] Hiroki Takesue,[2] Toshimori Honjo,[2] Kyo Inoue,[2] and Yoshihisa Yamamoto[1,2]
[1]*Edward L. Ginzton Laboratory, Stanford University, Stanford, California 94305, USA*
[2]*NTT Basic Research Laboratories, NTT Corporation, Kanagawa 243-0198, Japan*

(Received 7 June 2005; revised manuscript received 9 August 2005; published 11 November 2005)

We compare the performance of various quantum-key-distribution (QKD) systems using a single-photon detector, which combines frequency up-conversion in a periodically poled lithium niobate waveguide and a silicon avalanche photodiode (APD). The comparison is based on the secure communication rate as a function of distance for three QKD protocols: the Bennett-Brassard 1984, the Bennett-Brassard-Mermin 1992, and the coherent differential-phase-shift keying protocols. We show that the up-conversion detector allows for higher communication rates and longer communication distances than the commonly used InGaAs/InP APD for all three QKD protocols.

DOI: 10.1103/PhysRevA.72.052311 PACS number(s): 03.67.Dd, 42.65.−k

I. INTRODUCTION

Quantum key distribution (QKD) allows two parties to share an unconditionally secure secret key. Security is guaranteed by the laws of quantum mechanics, ensuring that the key can be used afterward to encrypt and decrypt secret messages as a one-time pad. The most common QKD protocols, which have been implemented in experiments over recent years [1], are the Bennett-Brassard 1984 (BB84) protocol, which uses single photons as information carriers [2], and the entanglement-based Bennet-Brassard-Mermin 1992 (BBM92) protocol [3]. A security analysis for these protocols under realistic system parameters and against individual attacks has been performed [4,5]. This analysis shows that the performance of a quantum-cryptography system, in terms of communication distance and secure communication rate, is determined by the characteristics of the source of single or entangled photons, and of the single-photon detectors. In addition to the BB84 and BBM92 protocols, we consider the recently proposed differential-phase-shift keying (DPSK) protocol, which uses a weak coherent pulse train as the information carrier [6,7]. To this end, we develop a security analysis against certain types of hybrid attacks.

To date, fiber-optic QKD systems have invariably used InGaAs/InP avalanche photodiodes (APDs) as single-photon detectors. Recently, an alternative technology for very efficient single-photon detection at 1.55 μm, based on the principle of frequency up-conversion, was presented [8]. Using realistic experimental parameters, we perform comparisons for the various types of sources and protocols, and show that longer communication distances and higher communication rates can be achieved using the up-conversion detector in all cases.

II. 1.55-μm SINGLE-PHOTON DETECTORS

A. InGaAs/InP avalanche photodiode

The InGaAs/InP avalanche photodiodes have been the subject of thorough investigation over the last decade due to their importance as single-photon detectors in fiber-optic QKD implementations. Although considerable progress has been achieved in the performance of these detectors [9–13], they exhibit low quantum efficiencies (typically on the order of 0.1), and, most seriously, they suffer from after-pulse effects caused by trapped charge carriers, which produce large dark-count rates during a relatively long time. The high dark-count probability imposes *gated-mode operation*, which limits their capabilities significantly. In particular, when operated in gated mode, the APD device is raised above breakdown threshold for a few nanoseconds, which ensures low probability of a dark count and high efficiency for detecting light. Subsequently, the device is returned to below breakdown for a time long enough for any trapped charge carrier to leak away. Given that the trapping lifetime is on the order of a microsecond, this mode allows operation at megahertz rates, while the after-pulse probability is reduced by the ratio of the gate width to the time separation between gates. In a QKD application, this gate frequency determines the repetition rate of the signal pulse and, therefore, limits the attainable communication rate. Furthermore, the dark-count rate, which is critical for the communication distance, is determined by the gate width, limited by the response time of the semiconductor material. Typically, gate widths of 1–2 ns at ~1 MHz repetition frequency are used with resulting dark counts on the order of 10^{-5}/gate.

B. Up-conversion detector

In the 1.55-μm up-conversion single-photon detector [8], a single photon at 1.55 μm interacts with a strong pump at 1.32 μm in a periodically poled lithium niobate (PPLN) waveguide, designed for sum-frequency generation at these wavelengths [14]. Due to the quasi-phase-matching and the tight mode confinement over long interaction lengths achieved in a guided-wave structure, this device allows for very high conversion efficiency of the signal to the ~0.7-μm sum-frequency output. The converted photon is subsequently detected by a silicon APD. Contrary to InGaAs/InP APDs, Si APDs have high quantum efficiencies

[*] Electronic address: ediam@stanford.edu

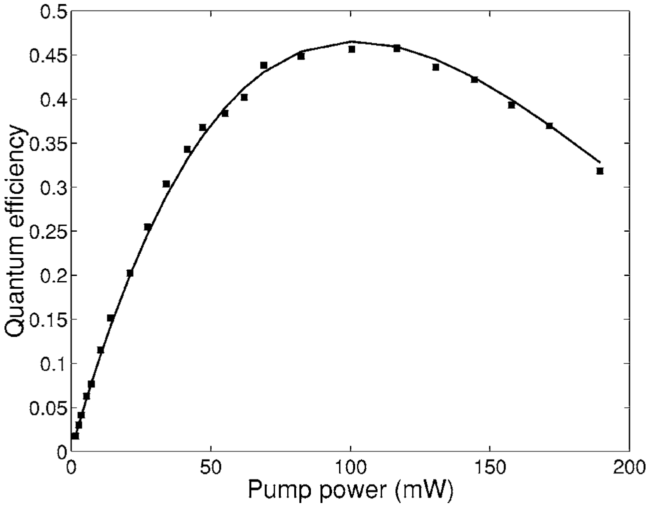

FIG. 1. Quantum efficiency of the 1.55-μm up-conversion single-photon detector as a function of pump power. The expression for the fitting curve is given by Eq. (1).

in the near infrared (typically on the order of 0.6–0.7), very low dark-count rates, and very small after-pulse effects. The last characteristic enables *Geiger (nongated) mode operation* of the Si APD, which does not impose any severe limitation on the attainable communication rate in a QKD system. In practice, however, the rate is limited by the dead time of Si APD detectors, which is on the order of 50 ns for commercial devices. During this time period that follows a photodetection event, the photodiode cannot respond to subsequent events, and, eventually, a very large photon flux saturates the device. This effect is taken into account in the calculations of Sec. IV.

The main characteristics of the up-conversion detector, such as the quantum efficiency η_{up} and the dark-count rate D_{up}, depend on the pump power p [8]. When the phase-matching condition in the waveguide is met and sufficient pump power is available to achieve almost 100% photon conversion, a maximum overall quantum efficiency of 0.46 is achieved, as shown in Fig. 1. In agreement with the coupled-mode theory for three-wave interactions in a waveguide, which predicts a $\sin^2$ dependence of η_{up} on p, the fitting curve of the experimental results is given by the following expression:

$$\eta_{\text{up}}(p) = a_1 \sin^2(\sqrt{a_2 p}) \tag{1}$$

where a_1=0.465, a_2=79.75, and p is given in mW.

On the other hand, we believe that the dark-count rate is dominated by the following combined nonlinear process. Initially, the pump photons are scattered by the phonons of both the PPLN waveguide and the fiber via a spontaneous Raman scattering process. This process scales linearly with the pump power, and generates a spectrum of Stokes photons, which includes the signal wavelength of 1.55 μm. Subsequently, the noise photons interact with the pump photons in the waveguide via the phase-matched sum-frequency generation process, and create dark counts. The combined process results in an approximately quadratic dependence of the dark counts on the pump power, as shown in Fig. 2. A more accurate polynomial fitting curve is given by the following expression:

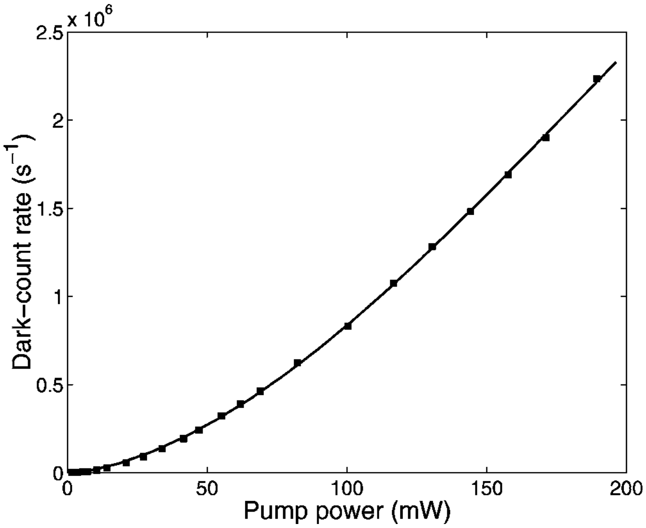

FIG. 2. Dark-count rate of the 1.55-μm up-conversion single-photon detector as a function of pump power. The expression for the fitting curve is given by Eq. (2).

$$D_{\text{up}}(p) = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + b_4 p^4 \quad (\text{s}^{-1}) \tag{2}$$

where b_0=50, b_1=826.4, b_2=110.3, b_3=−0.403, b_4 =0.000 65, and p is again given in mW. Another possible origin of dark counts is a potentially phase-matched parametric fluorescence process, followed by up-conversion of the noise signal photons [15,16]. This process would also invoke a quadratic dependence of the dark counts on the pump power. However, the strong absorption in lithium niobate of the 8.9-μm idler photons associated with such a parametric fluorescence process in the up-conversion detector described here suggests that the combined process involving spontaneous Raman scattering described above dominates the generation of dark counts. This conclusion is also supported by the fact that by interchanging the pump and signal wavelengths the dark counts are significantly reduced [8], which can be explained by the smaller anti-Stokes scattering gain due to the thermal occupation factor of the excited vibrational states in the waveguide device.

An important feature of the up-conversion detector stems from the fact that the dark counts depend on the bandwidth of the waveguide, as this determines the number of noise photons. We can define a quantity $D_{\text{up Hz}}$=$D_{\text{up}}/B_{\text{d}}$ s^{-1} Hz^{-1} for a detector with bandwidth B_{d}, which corresponds to the dark counts per mode. Then, we can think of the ideal communication system shown in Fig. 3 with a matched filter with bandwidth equal to the bit rate B, and a measurement time window equal to $1/B$. In such a system, the dark counts per time window, d_{up}, a parameter of great importance in QKD applications, is equal to $D_{\text{up Hz}}$. Note that d_{up} is independent of the bit rate B (or measurement time window $1/B$) under this optimum filtering. In the case of an InGaAs/InP APD operated in gated mode, the gate width is equal to $1/B$ and thus the dark counts per gate, d_{APD}, is calculated by D_{APD}/B,

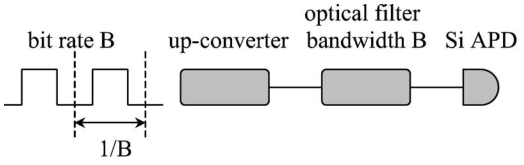

FIG. 3. Ideal communication system employing an up-conversion detector.

where D_{APD} (s^{-1}) is the dark-count rate of the InGaAs/InP APD. Table I summarizes the definitions of the dark-count quantities that we have introduced. In Fig. 4, the quantities d_{up} and d_{APD} are plotted as functions of the bit rate. For the InGaAs/InP APD, the typical value $D_{\mathrm{APD}}=10^4\ \mathrm{s}^{-1}$ is used. For the up-conversion detector, we calculate the quantity $D_{\mathrm{up\ Hz}}$ at the operating point of the detector, where the normalized noise equivalent power (NEP) $\sqrt{2D_{\mathrm{up}}}/\eta_{\mathrm{up}}$ is minimized, which corresponds to $D_{\mathrm{up}}=6.4\times10^3\ \mathrm{s}^{-1}$ and $\eta_{\mathrm{up}}=0.075$. Given a bandwidth of $B_{\mathrm{d}}=50$ GHz for the up-converter, we find that the optimum d_{up} is $\sim1.3\times10^{-7}$, as shown in Fig. 4. This result illustrates the significant advantage of the up-conversion detector for most practical system bit rates.

The dependence of the dark counts on the waveguide bandwidth, together with the nongated mode operation of the Si APD and the pump power dependence of the detector characteristics, have a significant effect on the performance of a quantum-cryptography system employing up-conversion detectors, as we will see in the following sections.

III. COMMUNICATION RATE EQUATIONS

In this paper, we will consider only individual attacks, that is, Eve is restricted to attack only individual bits; she is not allowed to perform a coherent attack consisting of collective quantum operations and measurements of many qubits with quantum computers. In a QKD system, the raw transmission of random bits is followed by a public exchange of information on the time of single-photon detection and the bases used by the two parties, which results in the *sifted key*. The steps of classical error correction and privacy amplification follow. The first step serves the dual purpose of correcting all erroneously received bits and giving an estimate of the error rate. Privacy amplification is then used to distill a shorter key, the *final key*, which can be made as secure as desired. The security analysis of [4,5] takes all the above steps into account and derives the communication rate equations that are restated in Secs. III A and III B. In Sec. III C, we derive the corresponding equation for the DPSK protocol, based on the security analysis against certain types of hybrid attacks.

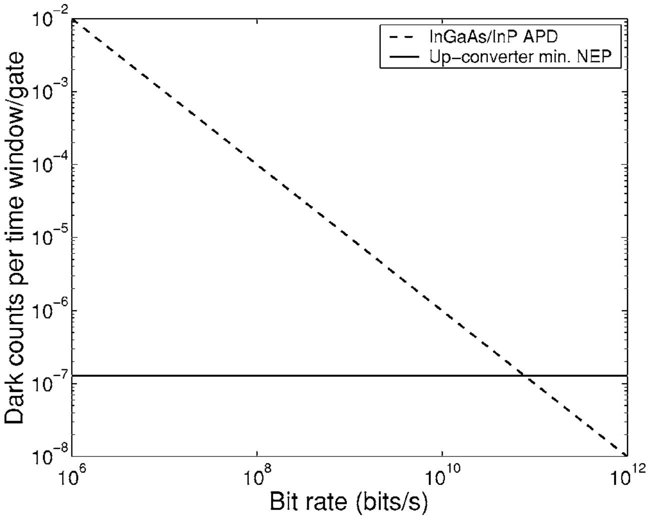

FIG. 4. Dark counts per time window/gate for the up-conversion single-photon detector operating at the minimum NEP regime, and a typical InGaAs/InP APD, respectively, in the communication system described in Fig. 3.

A. BB84 protocol

In the BB84 protocol, Alice sends Bob single photons randomly modulated in two nonorthogonal bases. Bob measures the polarization states of the single photons in a randomly chosen polarization basis. The secure communication rate of this protocol against an arbitrary individual attack, including the most commonly considered intercept-resend and photon-number splitting (PNS) attacks [4], is given by the following expression:

$$R_{\mathrm{BB84}}=\frac{1}{2}\nu p_{\mathrm{click}}\{\tau(e,\beta)+f(e)[e\log_2 e+(1-e)\log_2(1-e)]\}. \tag{3}$$

In the above equation, the factor $\frac{1}{2}$ is called the sifting parameter and is due to the fact that Alice's and Bob's polar-

TABLE I. Definitions of the dark-count quantities for the up-conversion detector and the InGaAs/InP APD.

	Up-converter	InGaAs/InP APD
Dark count rate (s^{-1})	D_{up}	D_{APD}
Dark counts per mode ($\mathrm{s}^{-1}\ \mathrm{Hz}^{-1}$)	$D_{\mathrm{up\ Hz}}=\frac{D_{\mathrm{up}}}{B_{\mathrm{d}}}$ [a]	-
Dark counts per time window/gate	$d_{\mathrm{up}}=D_{\mathrm{up\ Hz}}$	$d_{\mathrm{APD}}=D_{\mathrm{APD}}\frac{1}{B}$ [b]

[a] B_{d} is the waveguide bandwidth.

[b] B is the bit rate.

TABLE II. Benchmark performance of the error-correction algorithm given in [17].

e	$f(e)$
0.01	1.16
0.05	1.16
0.1	1.22
0.15	1.35

ization bases are not the same with probability $\frac{1}{2}$. The repetition rate of the transmission is given by ν. The probability that Bob detects a photon is

$$p_{\mathrm{click}} = p_{\mathrm{signal}} + p_{\mathrm{dark}}. \tag{4}$$

Simultaneous signal and dark counts are ignored in the above expression, and the two components are given by

$$p_{\mathrm{signal}} = \mu \eta \, 10^{-(\alpha L + L_{\mathrm{r}})/10}, \tag{5}$$

$$p_{\mathrm{dark}} = 4d, \tag{6}$$

where μ is the average number of photons per pulse, η the quantum efficiency of the detector, α the loss coefficient of the optical fiber in dB/km, L the distance in km, L_{r} the loss of the receiver unit in dB, and d the dark counts per measurement time window of the system. The coefficient 4 in Eq. (6) is due to the assumption of a passive detection unit involving four detectors at Bob's site, as in [5]. For an ideal single-photon source, $\mu=1$, while for a Poisson source, which corresponds to the common weak laser pulse implementations [1], μ becomes a free variable which should be optimized.

The error rate is given by the expression:

$$e = \frac{\frac{1}{2}p_{\mathrm{dark}} + b p_{\mathrm{signal}}}{p_{\mathrm{click}}} \tag{7}$$

where b is the baseline system error rate, which cannot be distinguished from tampering. The last term in Eq. (3) corresponds to the additional shrinking of the sifted key due to the leakage of information to Eve during classical error correction. The function $f(e)$ depends on the error-correction algorithm and its values are given in Table II for the bidirectional algorithm developed in [17].

Finally, the main shrinking factor $\tau(e,\beta)$ in the privacy amplification step is related through the expression

$$\tau = -\log_2 p_{\mathrm{c}} \tag{8}$$

to the average collision probability p_{c}. This is a measure of Eve's mutual information with Alice and Bob. In [4] the following result is derived for τ:

$$\tau(e,\beta) = -\beta \log_2\left[\frac{1}{2} + 2\frac{e}{\beta} - 2\left(\frac{e}{\beta}\right)^2\right]. \tag{9}$$

The parameter β is defined as the fraction of single-photon states emitted by the source:

$$\beta = \frac{p_{\mathrm{click}} - p_{\mathrm{m}}}{p_{\mathrm{click}}}, \tag{10}$$

where p_{m} is the probability that the source emits a multiphoton state. For an ideal single-photon source, $p_{\mathrm{m}}=0$ (i.e., $\beta=1$), while for a Poisson source,

$$p_{\mathrm{m}} = 1 - (1+\mu)e^{-\mu}. \tag{11}$$

Essentially, the parameter β accounts for the PNS attacks, with which Eve can obtain full information without causing any error in the communication between Alice and Bob by performing a quantum nondemolition measurement of the photon number in each pulse, keeping one photon in her quantum memory when she detects multiple photons, and applying a delayed measurement on her photon after the public announcement of the bases by Bob. This attack is a major restricting factor in the performance of a weak laser pulse implementation of the BB84 protocol. The secure communication rate decreases quadratically with the transmission of the quantum channel, $10^{-\alpha L/10}$, for small error rate and $p_{\mathrm{dark}} \ll p_{\mathrm{signal}} \ll 1$. On the contrary, for an ideal single-photon source implementation, under the same conditions we find $R_{\mathrm{BB84}} \approx \frac{1}{2}\nu p_{\mathrm{signal}}$, i.e., the rate decreases only linearly with the fiber transmission.

The above security analysis is based on the assumption that Eve has a quantum memory with an infinitely long coherence time because Alice and Bob can delay the public announcement for an arbitrarily long time. If Eve is not equipped with such a quantum memory, she must perform the polarization measurement with a randomly chosen basis. In this realistic case, Eq. (9) must be modified to

$$\tau(e,\beta) = -\frac{1+\beta}{2}\log_2\left[\frac{1}{2} + 4\frac{e}{1+\beta} - 8\left(\frac{e}{1+\beta}\right)^2\right]. \tag{12}$$

Recent studies have shown that modifications of the BB84 protocol, such as changing the sifting procedure [18], or introducing decoy states [19–21], can make the protocol a lot more robust against PNS attacks and, consequently, extend the secure key-distribution distance of BB84 with Poisson sources significantly. Although a detailed analysis of these variations is beyond the scope of this paper, we will consider the vacuum+weak decoy state protocol described in [20] in our comparison in Sec. IV.

B. BBM92 protocol

The BBM92 protocol is the two-photon variant of BB84. Alice and Bob each share a photon of an entangled photon pair, for which they measure the polarization state in a randomly chosen basis out of two nonorthogonal bases. It was shown in [5] that the average collision probability p_{c} for this protocol is the same as that of the BB84 with a single-photon source, i.e., with $\beta=1$. The shrinking factor τ becomes:

$$\tau(e) = -\log_2\left(\frac{1}{2} + 2e - 2e^2\right). \tag{13}$$

This indicates that there is no analog to a photon-number splitting attack in BBM92. In general, the nature of this entanglement-based protocol renders it more robust than BB84; for example, it is less vulnerable to errors caused by dark counts, since one dark count alone cannot produce an error in this protocol. The equation for the secure communication rate against any individual attack is given by the following expression [5]:

$$R_{\mathrm{BBM92}} = \frac{1}{2}\nu p_{\mathrm{coin}}\{\tau(e) + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\}. \tag{14}$$

The sifting parameter is the same as in BB84, while the probability of a coincidence between Alice and Bob is

$$p_{\mathrm{coin}} = p_{\mathrm{true}} + p_{\mathrm{false}}. \tag{15}$$

The expressions for the probability of a true coincidence, p_{true}, and the probability of a false coincidence, p_{false}, are different for a deterministic entangled-photon source and a Poissonian entangled-photon source, such as a parametric down-converter (PDC). They are given below, under the assumption that the source is placed halfway between the two parties [5].

(1) Deterministic entangled-photon source,

$$p_{\mathrm{true}} = \eta^2\, 10^{-(\alpha L + 2L_{\mathrm{r}})/10}, \tag{16}$$

$$p_{\mathrm{false}} = 8d\eta\, 10^{-(\alpha L + 2L_{\mathrm{r}})/20} + 16d^2. \tag{17}$$

(2) Poissonian entangled-photon source,

$$p_{\mathrm{true}} = c_1, \tag{18}$$

$$p_{\mathrm{false}} = 16d^2 c_2 + 8dc_3 + c_4, \tag{19}$$

where

$$c_1 = \frac{1}{\cosh^4\chi}\frac{2t_L^2\tanh^2\chi}{[1-\tanh^2\chi(1-t_L)^2]^4}, \tag{20}$$

$$c_2 = \frac{1}{\cosh^4\chi}\frac{1}{[1-\tanh^2\chi(1-t_L)^2]^2}, \tag{21}$$

$$c_3 = \frac{1}{\cosh^4\chi}\frac{2t_L(1-t_L)\tanh^2\chi}{[1-\tanh^2\chi(1-t_L)^2]^3}, \tag{22}$$

$$c_4 = \frac{1}{\cosh^4\chi}\frac{4t_L^2(1-t_L)^2\tanh^4\chi}{[1-\tanh^2\chi(1-t_L)^2]^4}, \tag{23}$$

and

$$t_L = \eta\, 10^{-(\alpha L + 2L_{\mathrm{r}})/20}. \tag{24}$$

All the parameters in the above equations are defined as in the previous section. The parameter χ, which appears in the case of the Poissonian entangled-photon source, is a free variable that depends on the average photon-pair number per pulse, i.e., the nonlinear coefficient, the pump energy, and the interaction time of the down-conversion process. Finally, the error rate is given by the expression

$$e = \frac{\frac{1}{2}p_{\mathrm{false}} + b p_{\mathrm{true}}}{p_{\mathrm{coin}}}. \tag{25}$$

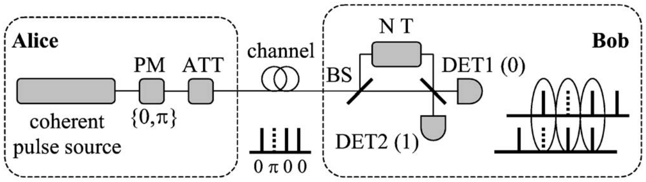

FIG. 5. Configuration of the DPSK protocol. PM, phase modulator; ATT, attenuator; BS, beam splitter; DET, detector.

For small error rate and $p_{\mathrm{false}} \ll p_{\mathrm{true}}$, the secure communication rate of BBM92 decreases linearly with the transmission of the quantum channel, similarly to the case of the BB84 protocol with a single photon source. Note that Eve does not need a quantum memory to attack the BBM92 protocol. Equation (14) is solely determined by the intercept and resend attack.

C. DPSK protocol

Instead of using two nonorthogonal bases as in BB84 and BBM92, the differential-phase-shift keying protocol uses many nonorthogonal states consisting of many pulses [6,7]. In particular, it is based on the fact that highly attenuated coherent states of many pulses with random $\{0,\pi\}$ phase modulation are mutually nonorthogonal. The idea of encoding the information in the phase of highly attenuated coherent pulses was first presented by Bennett in 1992 (B92) [22]. The DPSK protocol is a simpler but more efficient protocol compared to the B92 protocol. A similar protocol has also recently been proposed [23].

In the DPSK protocol, shown in Fig. 5, all pulses are highly attenuated and randomly phase modulated by $\{0,\pi\}$. Each photon coherently spreads over many pulses with a fixed phase modulation pattern. In the receiver side, Bob randomly modulates the delay time NT in his interferometer by randomly choosing a positive integer N, as shown in Fig. 5, where T is the inverse of the clock frequency. After passing through Bob's interferometer, the pulses interfere at Bob's output beam splitter, and which detector clicks depends on the phase difference of the two pulses separated by a time NT. Bob announces publicly the time instances at which a photon was detected and the randomly chosen positive integer N. From her modulation data Alice knows which detector recorded the event. Thus, they form a secret key by assigning a bit value to each detector. The sifting parameter is 1 since all bits are utilized during the key formation.

The security of the DPSK protocol stems from the fact that the information is encoded on the differential phase of two nonlocal pulses. This renders the protocol robust against any type of individual photon splitting attack [24,25]. In order to derive the communication rate equation, we need to calculate the privacy amplification shrinking factor τ defined in Eq. (8) as a function of the average collision probability p_{c}. Our analysis takes into account a hybrid attack, which consists of two types of collective attacks.

1. Beam-splitter attack

Eve uses a beam splitter with transmission η_{BS} to obtain coherent copies of the quantum state of many pulses that

Alice sends to Bob. She also replaces the lossy optical fiber with a lossless one, and the inefficient detectors at Bob's receiver unit with ideal ones. Without Eve's intervention, Bob's probability of detecting a signal photon, p_{signal}, is identical to the one given in Eq. (5). In order to leave this probability unaltered, Eve has to set the beam-splitter transmission η_{BS} to

$$\eta_{\text{BS}} = \eta\, 10^{-(\alpha L + L_{\text{r}})/10} \tag{26}$$

where all the parameters are defined as in Sec. III A. One possibility for Eve is to measure the pulses that she picks up with an interferometer with delay time $M\tau$ chosen independently from Bob's. In this case, her information gain is calculated as follows. The probability of a detection event at Eve's and Bob's site at a given time slot is given by $\mu(1-\eta_{\text{BS}})$ and $\mu\eta_{\text{BS}}$, respectively, where μ is the average number of photons per pulse. Thus, the probability of a detection event at the same time instance is equal to $\mu^2\eta_{\text{BS}}(1-\eta_{\text{BS}})$. This means that the probability that Eve obtains the value of a bit at a certain time given that Bob has detected a photon at that time is given by $\mu^2\eta_{\text{BS}}(1-\eta_{\text{BS}})/\mu\eta_{\text{BS}}=\mu(1-\eta_{\text{BS}})$. On the other hand, the probability that Eve's randomly chosen M matches Bob's N is equal to $1/N$. Thus, the probability that Eve gains bit information relative to Bob is $\mu(1-\eta_{\text{BS}})/N$. This is true if we assume that Eve is not equipped with a quantum memory with an infinitely long coherence time. However, if we allow Eve to have a quantum memory, her strategy can be changed in order to increase her information gain. In this case, she keeps the pulses in her quantum memory and waits for Bob's announcement. Note that Alice and Bob can delay the public announcement for an arbitrarily long time, so Eve's quantum memory must have an infinitely long coherence time. Then, Eve uses an interferometer with an optical switch instead of a 50:50 beam splitter at the input side, which allows her to interfere only the pulses for which she is aware that Bob has obtained the differential phase information. This strategy increases Eve's probability of gaining bit information to $2\mu(1-\eta_{\text{BS}})$. The beam-splitter attack does not cause any error in the communication between Alice and Bob, hence it gives full information, i.e., $p_{\text{c}}=1$, to Eve for a fraction of bits equal to $\mu(1-\eta_{\text{BS}})/N$ or $2\mu(1-\eta_{\text{BS}})$. The remaining fraction of the bits is given by

$$\gamma = \begin{cases} 1 - \dfrac{\mu(1-\eta_{\text{BS}})}{N} = 1 - \dfrac{\mu}{N} + \dfrac{p_{\text{signal}}}{N} & \text{without quantum memory} \\ 1 - 2\mu(1-\eta_{\text{BS}}) = 1 - 2\mu + 2p_{\text{signal}} & \text{with quantum memory} \end{cases} \tag{27}$$

2. Intercept-resend attack

Eve also applies an intercept and resend attack to some of the pulses that are sent to Bob after her beam splitter. In particular, Eve intercepts two pulses with a time interval MT, lets them pass through an interferometer with an identical delay MT, measures the differential phase, and according to her measurement result she sends an appropriate state to Bob. We assume that in the case of an inconclusive or vacuum outcome she sends the vacuum state, while when she measures a single photon she sends a photon split into two pulses with the correct phase difference applied between them. In this case, when Bob picks up an identical delay, $N=M$, and measures the central time slot, he does not detect the eavesdropping because he obtains the correct answer. However, with probability $1-1/2N$ he chooses another delay, $N\neq M$, or measures the side time slots, which yield random, uncorrelated results, and with probability $\frac{1}{2}$ these lead to error. Hence, this attack causes a bit error of $\frac{1}{2}(1-1/2N)$ in the communication between Alice and Bob. If the error rate of the system is e, Eve is allowed to apply her attack to a fraction $2e/(1-1/2N)$ of the pulse pairs in order not to exceed this error rate. With probability $1/2N$, she obtains full information for these intercepted pulse pairs.

In summary, taking into account the hybrid attack consisting of the beam-splitter and intercept-resend attacks, we find that the fraction of bits for which Eve has no information, i.e., for which $p_{\text{c}}=\frac{1}{2}$, is equal to $\gamma - e/N(1-1/2N)$. Thus, we have calculated the privacy amplification shrinking factor,

$$\tau(e,\gamma) = \gamma - \frac{e}{N(1-1/2N)} \tag{28}$$

where γ is given by Eq. (27). We can now write the equation for the secure communication rate of the DPSK protocol against the hybrid attack we considered:

$$R_{\text{DPSK}} = \nu p_{\text{click}}\{\tau(e,\gamma) + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\}. \tag{29}$$

In the above equation, ν is the repetition rate of the transmission. The probability that Bob detects a photon, p_{click}, is defined in Eq. (4). The probability of a signal count, p_{signal}, is given by Eq. (5), while the probability of a dark count, p_{dark}, in this case is given by the expression

$$p_{\text{dark}} = 2d \tag{30}$$

because there are two detectors at the receiver unit. Finally, the error rate is defined in Eq. (7), and the values of $f(e)$ are given in Table II.

In the case of small error rate and $p_{\text{dark}} \ll p_{\text{signal}} \ll 1$, Eq. (29) gives $R_{\text{DPSK}} \approx \nu(1-\mu/N)p_{\text{signal}}$ without a quantum memory, or $R_{\text{DPSK}} \approx \nu(1-2\mu)p_{\text{signal}}$ with a quantum memory. This means that the secure rate for the DPSK protocol decreases linearly with the fiber transmission. This is in agreement with the results of [23,26], who have considered a protocol similar to DPSK and a slightly modified B92 protocol, respectively.

IV. NUMERICAL RESULTS

We compare the performance of quantum-key-distribution systems implementing the BB84, BBM92, and DPSK protocols, when the up-conversion single-photon detector is used. In order to do that, we calculate the secure communication rate as a function of distance for fiber-optic implementations of the three protocols, based on Eqs. (3), (14), and (29), respectively. In the case of BB84 and BBM92, both ideal and realistic sources of single and entangled photons are considered. Some parameters are fixed in all simulations: the channel loss is set to $\alpha=0.2$ dB/km at 1.55 μm, the baseline system error rate is set to $b=0.01$, and in addition to the fiber losses we assume an extra loss of $L_{\text{r}}=1$ dB at the receiver site. As mentioned in Sec. III A, in the case of a weak-laser-pulse implementation of the BB84 protocol, the average number of photons per pulse, μ, is an adjustable parameter, with respect to which the rate is numerically optimized at each distance. Intuitively, such optimization is necessary because when this parameter is too low the dark counts dominate, while when it is too high the probability of multiphoton pulses becomes very large. In both cases, secure communication quickly becomes impossible. The rate is optimized with respect to μ in the case of the DPSK protocol as well, while the corresponding adjustable parameter is χ in the case of the BBM92 protocol with a Poissonian entangled-photon source.

It is clear from the analysis of Sec. III that the critical parameters for the performance of a quantum-cryptography system related to the single-photon detector employed are the dark counts per measurement time window, d, the quantum efficiency η, and the repetition rate of the transmission that it allows, ν. In the case of the up-conversion single-photon detector, due to the nongated-mode operation of the Si APD there is no severe limitation to the repetition rate of the experiment. In practice, the limit is set by the speed of the electronic equipment as well as by the timing jitter of the Si APD (typically 0.5–0.7 ns). A realistic value, compatible with currently available components, is $\nu_{\text{up}}=1$ GHz. As was explained in Sec. II B, the limiting factor for the attainable communication rate is the dead time of the Si APD, t_{d}. Assuming that the photodetection events follow a Poisson process, the probability of two events occurring in a time period larger than t_{d} is given by the exponential factor $e^{-\delta\nu p_{\text{click}}t_{\text{d}}}$, where δ depends on the number of detectors in the receiver unit. For the typical value $t_{\text{d}}=50$ ns, this saturation factor becomes rather small at rates greater than a few megahertz, limiting the final rate at small fiber losses. Using Eqs. (1) and (2), we numerically optimize the communication rate for each protocol with respect to the pump power p at each distance. Such optimization is intuitively necessary because depending on the communication distance an equilibrium between the values of the quantum efficiency and the dark counts of the up-conversion detector has to be established. The result of this optimization indicates the optimal regime of operation of the detector at each distance. Finally, the optimum filtering configuration, shown in Fig. 3, is assumed, which sets the measurement time window to 1 ns.

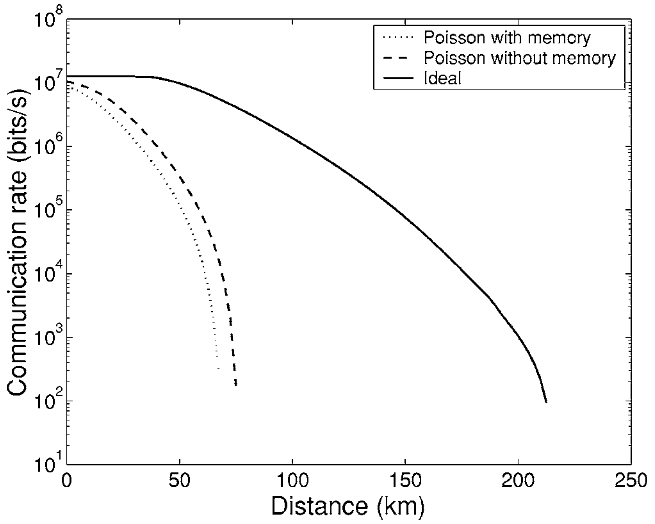

FIG. 6. Secure communication rate as a function of distance for the BB84 protocol employing a Poisson or an ideal single-photon source.

The simulation results are shown in Figs. 6, 7, and 8 for the BB84, BBM92, and DPSK protocols, respectively. Each curve features a cutoff distance, which is due to the increasing contribution of the dark counts with fiber length. The saturation effect, related to the dead time of the Si APD, is apparent for small fiber losses and high bit rates.

In the case of the BB84 with a Poisson single-photon source, we observe in Fig. 6 that not allowing Eve to possess a quantum memory with an infinitely long coherence time does not have a major effect on the performance of the system. The quadratic decrease of the rate of the communication rate with the fiber length, a consequence of the PNS attacks,

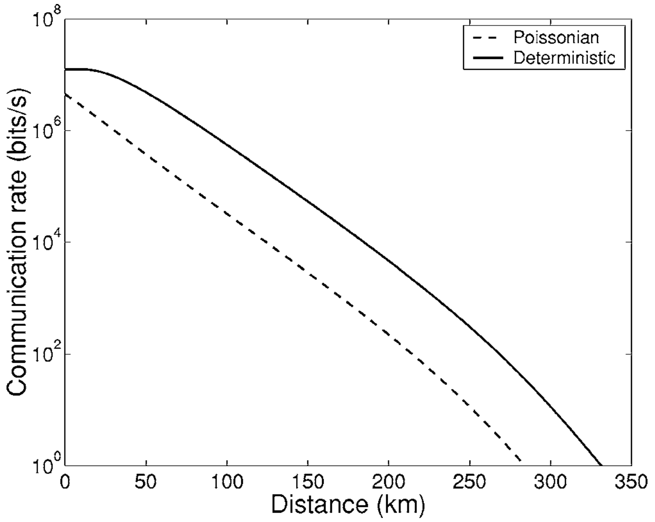

FIG. 7. Secure communication rate as a function of distance for the BBM92 protocol employing a Poissonian or a deterministic entangled-photon source.

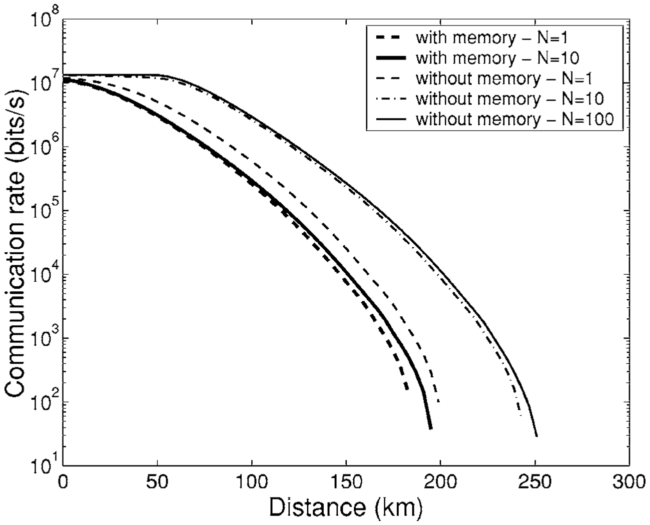

FIG. 8. Secure communication rate as a function of distance for the DPSK protocol employing time delay parameters $N=1$ or 10 when Eve is equipped with a quantum memory and $N=1$, 10, or 100 when she is not.

is a dominant factor, making this implementation of the standard BB84 protocol unsuitable for long-distance quantum cryptography. On the contrary, the use of an ideal single-photon source allows for a significantly longer communication distance with high communication rates. However, such a source does not exist today at 1.55 μm, although efforts toward this goal are under way [27].

As shown in Fig. 7, the inherently more robust entanglement-based BBM92 protocol allows for even longer communication distances, having the capability to achieve a practical 1-Hz secure key-generation rate at more than 300 km with a deterministic entangled-photon source. However, technological difficulties related to entanglement generation and coincidence detection at 1.55 μm have until today limited this distance to 30 km [28].

The DPSK protocol features characteristics very similar to BB84 with a single-photon source, due to its robustness to PNS attacks, as was shown in the security analysis of Sec. III C. When Eve is equipped with a quantum memory, we observe in Fig. 8 that introducing a time delay parameter N does not have a significant effect on the performance of the system, since the beam-splitter attack term in Eq. (28), which is independent of N in this case, dominates. However, when a realistic scenario is assumed, where Eve does not possess a quantum memory with an infinitely long coherence time, we observe a significant effect on the performance of the system. Indeed, in this case introducing a time delay parameter N greater than 1 enhances both the secure communication rate and the communication distance of the system considerably. Nevertheless, the advantage becomes comparatively smaller as N increases to values greater than 10. This result shows that the DPSK protocol is a very practical and appealing alternative for a long-distance QKD system, with the potential of 1-kHz secure key-generation rate over distances longer than 200 km.

For all the QKD protocols, if instead of the up-conversion detector we assume an InGaAs/InP APD with $\nu_{\mathrm{APD}}=10$ MHz, which is the best gate frequency achieved to date [9], and the typical values $\eta_{\mathrm{APD}}=0.1$ and $d_{\mathrm{APD}}=10^{-5}$/gate [23], we find that the maximum communication distance is about half of the one achieved with an up-conversion detector, while the communication rate is two orders of magnitude lower than with the up-conversion detector, due to the gated-mode operation of the InGaAs/InP APD. Clearly, the up-conversion detector offers a great advantage over the InGaAs/InP APD as a single-photon detector in a QKD system, in terms of both secure communication rate and communication distance.

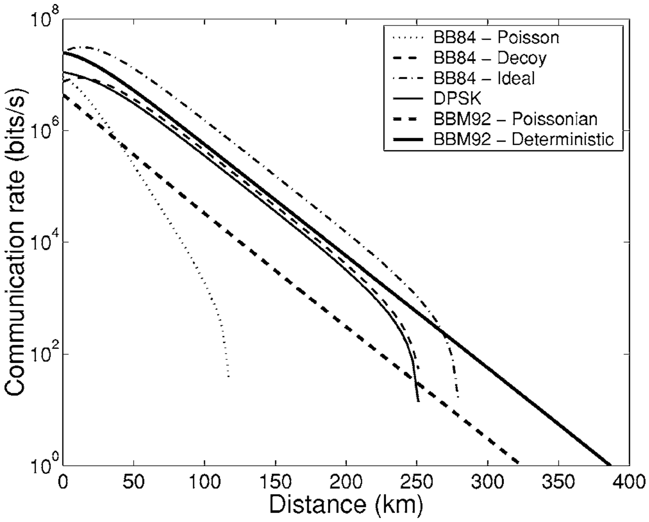

FIG. 9. Comparison of the performance of QKD systems implementing the BB84, BBM92, and DPSK protocols. In all cases it is assumed that Eve is equipped with an ideal quantum memory and that an optimized up-conversion single-photon detector is used. For the DPSK protocol $N=1$. For the decoy state protocol the average number of photons per pulse of the signal states, μ, is determined by the baseline system error rate, $b=0.01$, and is set to 0.77, while the average number of photons per pulse of the weak decoy state is set to 0.05 [20].

Finally, in Fig. 9 we compare the performance of quantum-key-distribution systems implementing the three protocols, under the assumptions that Eve is equipped with an ideal quantum memory and that the dark counts of the up-conversion detector, caused by parasitic nonlinear processes in the PPLN waveguide, are eliminated. This means that the detector's performance is ideally limited by the Si APD characteristics, which corresponds to $d_{\mathrm{up}}=5\times10^{-8}$. Operation at the maximum quantum efficiency regime is also assumed, i.e., $\eta_{\mathrm{up}}=0.46$. In our comparison we also include the vacuum+weak decoy state protocol described in [20]. We observe that, ultimately, 250 km of secure communication distance is possible with the DPSK protocol and the BB84 protocol with decoy states. An ideal single-photon source implementation of BB84 can extend this distance even more, while BBM92 has the potential of reaching 350 km of secure key distribution with a deterministic entangled-photon source.

V. CONCLUSIONS

In this paper, we studied the main characteristics of two types of 1.55-μm single-photon detectors, the InGaAs/InP

APD and the up-conversion detector, which combines frequency up-conversion in a PPLN waveguide and detection by a silicon APD. We presented the communication rate equations for the BB84 and the BBM92 QKD protocols, and we derived a corresponding equation for the DPSK protocol, developing a security analysis of this protocol against certain types of hybrid attacks. Based on these equations, we compared the performance of fiber-optic quantum-key-distribution systems employing the protocols under consideration, with realistic experimental parameters. In all cases, we found that a secure communication rate of two orders of magnitude higher than before is possible, while the use of the up-conversion detector enables quantum key distribution over communication distances longer by a factor of 2 than with an InGaAs/InP APD. Furthermore, the importance of the implemented protocol was illustrated, and the impact of Eve's allowed capabilities was investigated. We concluded that the simple and efficient DPSK protocol allows for more than 200 km of secure communication distance with high communication rates, in the realistic case that Eve does not possess a quantum memory with an infinitely long coherence time, and the time delay parameter N is greater than 1. The BB84 protocol with decoy states, a practical and promising alternative, achieves a similar performance. Finally, the BBM92 protocol can extend the secure key-distribution distance to 300 km with a reasonably high secure key-generation rate. It is clear that improving the performance of the Si APDs with respect to their dead time and timing jitter and reducing the dark counts of the up-converter will extend the capabilities of fiber-optic QKD systems employing these protocols even further. In addition to improvements in the detection apparatus, solutions to problems resulting from the chromatic dispersion and birefringence in optical fibers, such as the use of dispersion-shifted fibers or dispersion compensation techniques [28] and phase-encoding protocols with small polarization-dependence interferometers [29], will be of major importance in practical quantum-cryptography systems, spanning hundreds of kilometers.

ACKNOWLEDGMENTS

The authors would like to thank Edo Waks for his helpful comments and suggestions. Financial support was provided by the MURI Center for Photonic Quantum Information Systems (ARO/ARDA Grant No. DAAD19-03-1-0199), and the Quantum Entanglement Project-SORST-JST.

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

[2] C. H. Bennett and G. Brassard, in *Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

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

[4] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[5] E. Waks, A. Zeevi, and Y. Yamamoto, Phys. Rev. A **65**, 052310 (2002).

[6] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).

[7] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).

[8] C. Langrock, E. Diamanti, R. V. Roussev, H. Takesue, Y. Yamamoto, and M. M. Fejer, Opt. Lett. **30**, 1725 (2005).

[9] A. Yoshizawa, R. Kaji, and H. Tsuchida, Jpn. J. Appl. Phys., Part 2 **43**, L735 (2004).

[10] D. S. Bethune, W. P. Risk, and G. W. Pabst, J. Mod. Opt. **51**, 1359 (2004).

[11] D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J. Rarity, and T. Wall, J. Mod. Opt. **48**, 1967 (2001).

[12] M. Bourennane, A. Karlsson, J. Ciscar, and M. Mathés, J. Mod. Opt. **48**, 1983 (2001).

[13] C. Gobby, Z. L. Yuan, and A. J. Shields, Electron. Lett. **40**, 1603 (2004).

[14] R. V. Roussev, C. Langrock, J. R. Kurz, and M. M. Fejer, Opt. Lett. **29**, 1518 (2004).

[15] A. V. Vandevender and P. G. Kwiat, J. Mod. Opt. **51**, 1433 (2004).

[16] M. A. Albota and F. N. C. Wong, Opt. Lett. **29**, 1449 (2004).

[17] G. Brassard and L. Salvail, in *Advances in Cryptology—EUROCRYPT'93*, edited by T. Hellseth, Lecture Notes in Computer Science Vol. 765 (Springer, Berlin, 1994), p. 410.

[18] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

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

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

[23] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, e-print quant-ph/0411022.

[24] K. Inoue and T. Honjo, Phys. Rev. A **71**, 042305 (2005).

[25] T. Honjo and K. Inoue, Opt. Lett. (to be published).

[26] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2005).

[27] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden, New J. Phys. **6**, 163 (2004).

[28] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden, Eur. Phys. J. D **30**, 143 (2004).

[29] T. Honjo, K. Inoue, and H. Takahashi, Opt. Lett. **29**, 2797 (2004).