Passive sources for the Bennett-Brassard 1984 quantum key distribution protocol with practical signals

Marcos Curty[1], Xiongfeng Ma[2], Hoi-Kwong Lo[3], and Norbert Lütkenhaus[2]
[1] *ETSI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Campus Universitario, E-36310 Vigo, Pontevedra, Spain*
[2] *Institute for Quantum Computing & Department of Physics and Astronomy, University of Waterloo, N2L 3G1 Waterloo, Ontario, Canada*
[3] *Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, M5S 3G4 Toronto, Ontario, Canada*

Most experimental realizations of quantum key distribution are based on the Bennett-Brassard 1984 (so-called BB84) protocol. In a typical optical implementation of this scheme, the sender uses an active source to produce the required BB84 signal states. While active state preparation of BB84 signals is a simple and elegant solution in principle, in practice passive state preparation might be desirable in some scenarios, for instance, in those experimental setups operating at high transmission rates. Passive schemes might also be more robust against side-channel attacks than active sources. Typical passive devices involve parametric down-conversion. In this paper, we show that both coherent light and practical single photon sources are also suitable for passive generation of BB84 signal states. Our method does not require any external-driven element, but only linear optical components and photodetectors. In the case of coherent light, the resulting key rate is similar to the one delivered by an active source. When the sender uses practical single photon sources, however, the distance covered by a passive transmitter might be longer than the one of an active configuration.

PACS numbers:

I. INTRODUCTION

The transmission of secret information over an insecure communication channel constitutes an essential resource in modern information society. Quantum key distribution (QKD) is a technique that allows two distant parties (typically called Alice and Bob) to establish a secure secret key despite the computational and technological power of an eavesdropper (Eve), who interferes with the signals [1]. This secret key is the main ingredient of the one-time-pad or Vernam cipher [2], the only known encryption method that can deliver information-theoretic secure communications.

Most experimental realizations of QKD are based on the so-called BB84 QKD scheme introduced by Bennett and Brassard in 1984 [3]. In a typical quantum optical implementation of this protocol, Alice sends to Bob phase-randomized weak coherent pulses (WCP) with usual average photon number of 0.1 or higher [4, 5]. These states can be easily generated using only standard semiconductor lasers and calibrated attenuators. Each light pulse may be prepared in a different polarization state, which is selected, independently and randomly for each signal, between two mutually unbiased bases, *e.g.*, either a linear (H [horizontal] or V [vertical]) or a circular (L [left] or R [right]) polarizations basis. On the receiving side, Bob measures each incoming signal by choosing at random between two polarization analyzers, one for each possible basis. Once this quantum communication phase is completed, Alice and Bob use an authenticated public channel to process their data and obtain a secure secret key. This last procedure, called key distillation, involves, typically, local randomization, error correction to reconcile Alice's and Bob's data, and privacy amplication to decouple their data from Eve [6]. A full proof of the security for the BB84 QKD protocol with WCP has been given in Refs. [7, 8]. The performance of this scheme can be improved further if the original hardware is slightly modified. For instance, one can use the so-called decoy-state method [9, 10], where Alice varies the mean photon number of each signal state she sends to Bob. The measurement results associated to different intensity settings allow the legitimate users to obtain a better estimation of the behavior of the quantum channel. This translates into an enhancement of the achievable secret key rate, which can now basically reach the performance of single photon sources (SPS).

The preparation of the BB84 signal states is usually realized by means of an active source. For simplicity, we will first consider polarization encoding. (Note that phase encoding is mathematically equivalent to polarization encoding. Later in this paper, we will also consider phase encoding.) There are two main configurations; they are illustrated in Fig. 1 as cases A and B. In the first one (case A in the figure), Alice uses four laser diodes, one for each possible BB84 signal [4]. These lasers are controlled by a random number generator (RNG) [11] that decides each given time which one of the 4 diodes is triggered. The second configuration (case B in the figure) uses only one single laser diode in combination with a polarization modulator which is controlled by a RNG [5]. This modulator can rotate the state of polarization

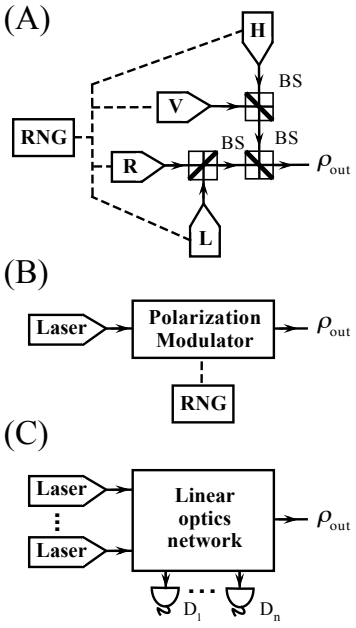

FIG. 1: (Case A) Example of an active setup with four laser diodes controlled by a random number generator (RNG). Each source emits one different BB84 signal state (*e.g.*, H [horizontal], V [vertical], L [circular left] or R [circular right] polarization states). BS denotes a beamsplitter. (Case B) Example of an active setup with one laser diode together with a polarization modulator controlled by a RNG. This modulator rotates the state of polarization of the incoming pulses to generate BB84 signal states. (Case C) Basic setup of a passive QKD transmitter with linear optics elements. One or more laser diodes produce different signal states that are sent through a linear optics network. Depending on the detection pattern observed in the detectors D_i, different signal states are actually generated. No RNG or active modulator are necessary in this last scenario.

of the signals produced by the source.

While active state preparation is a simple and elegant solution to implement the BB84 protocol in principle, in practice passive state preparation might be desirable in some scenarios [12–14]; for instance, in those experimental setups operating at high transmission rates, since no RNG is required in a passive device. A passive transmitter allows Alice to generate different quantum states at random without the need to use an external source of randomness. This situation is illustrated as case C in Fig. 1. Alice can use one or more light sources to produce different signal states that are sent through a linear optics network. Depending on the detection pattern observed in her detectors D_i, she can infer which signal states are actually generated. So far, only entanglement-based (EB) QKD systems have been designed to operate entirely in a passive regime without any external-driven elements [12, 15]. For instance, Alice and Bob can use a beamsplitter (BS) to passively and randomly select which bases to measure each incoming pulse. In

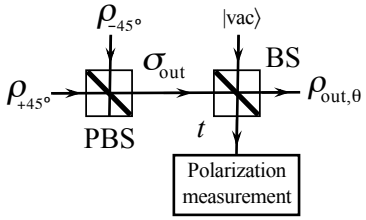

FIG. 2: Basic setup of a passive BB84 QKD source with strong coherent light. The mean photon number of the signal states $\rho_{+45°}$ and $\rho_{-45°}$ can be chosen very high; for instance, $\approx 10^8$ photons. The parameter t represents the transmittance of the BS; it satisfies $t \ll 1$.

this article, we show that both coherent light and practical SPS are also suitable for passive generation of BB84 signal states, *i.e.*, one does not need a nonlinear optics network preparing entangled states in order to passively generate BB84 signals. Practical SPS (also called "sub-Poissonian sources") are those light sources which have a smaller probability of emitting two or more photons than an attenuated laser. Our method requires only linear optical elements and photodetectors. In the asymptotic limit of an infinite long experiment, it turns out that the secret key rate of a passive source with coherent light is similar to the one delivered by an active source. When Alice uses practical SPS, however, the distance covered by a passive transmitter might be longer than the one of an active configuration. This result is caused by the capacity of the passive scheme to reduce the multiphoton probability of the source via a post-selection mechanism.

Passive schemes might also be more robust than active systems to side-channel attacks hidden in the imperfections of the optical components. If a polarization modulator is not properly designed, for example, it may distort some of the physical parameters of the pulses emitted by the sender depending on the particular value of the polarization setting selected. This fact could open a security loophole in the active schemes.

The article is organized as follows. In Sec. II we present and evaluate the performance of a passive BB84 state preparation scheme that can operate with coherent light. Then, in Sec. III we consider the case where Alice uses practical SPS. Finally, Sec. IV concludes the article with a summary. The paper includes as well a few appendixes with additional calculations.

II. PASSIVE TRANSMITTER WITH COHERENT LIGHT

The basic setup is rather simple. It is illustrated in Fig. 2. Suppose two phase-randomized strong coherent pulses prepared, respectively, in $+45°$ and $-45°$ linear polarization, interfere at a polarizing beamsplitter

(PBS). These states can be written as

$$\begin{aligned}\rho_{+45^\circ} &= e^{-\frac{\upsilon}{2}}\sum_{n=0}^{\infty}\frac{(\upsilon/2)^n}{n!}|n_{+45^\circ}\rangle\langle n_{+45^\circ}|,\\ \rho_{-45^\circ} &= e^{-\frac{\upsilon}{2}}\sum_{n=0}^{\infty}\frac{(\upsilon/2)^n}{n!}|n_{-45^\circ}\rangle\langle n_{-45^\circ}|,\end{aligned} \tag{1}$$

where $|n_{\pm 45^\circ}\rangle$ denote Fock states with n photons in $\pm 45^\circ$ linear polarization. The mean photon number, $\upsilon/2$, of each signal can be chosen very high; for instance, $\approx 10^8$ photons. In this scenario, we will show that the signal σ_{out} at the output port of the PBS can be expressed as

$$\sigma_{\text{out}} = \frac{1}{2\pi}e^{-\upsilon}\sum_{n=0}^{\infty}\frac{\upsilon^n}{n!}\int_\theta |n_\theta\rangle\langle n_\theta|\,\mathrm{d}\theta, \tag{2}$$

where the Fock states $|n_\theta\rangle$ are given by

$$|n_\theta\rangle = \frac{\left[\frac{1}{\sqrt{2}}\left(a^\dagger_{+45^\circ} + e^{i\theta}a^\dagger_{-45^\circ}\right)\right]^n}{\sqrt{n!}}|vac\rangle. \tag{3}$$

Here $|vac\rangle$ denotes the vacuum state, and $a^\dagger_{\pm 45^\circ}$ are the creation operators for the $\pm 45^\circ$ linear polarizations modes.

To see this, let us consider the interference of two pure coherent states with fixed phase relation and orthogonal polarizations, $|\sqrt{\upsilon/2}e^{i\phi_1}\rangle_{+45^\circ}$ and $|\sqrt{\upsilon/2}e^{i\phi_2}\rangle_{-45^\circ}$, at a PBS. The output signal is a coherent state of the form

$$|\sqrt{\upsilon}e^{i\phi_2}\rangle_\theta = e^{-\upsilon/2}\sum_{n=0}^{\infty}\frac{\left(\sqrt{\upsilon}e^{i\phi_2}\right)^n}{\sqrt{n!}}|n_\theta\rangle, \tag{4}$$

with $\theta = \phi_1 - \phi_2$. The case of two phase-randomized coherent pulses can be solved by just integrating the signal $|\sqrt{\upsilon}e^{i\phi_2}\rangle_\theta$ over all angles ϕ_2 and θ, *i.e.*,

$$\begin{aligned}\sigma_{\text{out}} &= \frac{1}{(2\pi)^2}\int_\theta\int_{\phi_2}|\sqrt{\upsilon}e^{i\phi_2}\rangle_\theta\langle\sqrt{\upsilon}e^{i\phi_2}|\,\mathrm{d}\phi_2\mathrm{d}\theta\\ &= \frac{1}{2\pi}e^{-\upsilon}\sum_{n=0}^{\infty}\frac{\upsilon^n}{n!}\int_\theta|n_\theta\rangle\langle n_\theta|\,\mathrm{d}\theta.\end{aligned} \tag{5}$$

Now, to prepare the signal states that are sent to Bob, Alice performs a polarization measurement followed by a post-selection step. By assumption, we have that the intensity υ of the signals σ_{out} is very high. Therefore, Alice can always employ, for instance, a BS of very small transmittance ($t \ll 1$) to split these states into two light beams: one very weak suitable for QKD, and one strong. The weak signal is sent to Bob through the quantum channel (see Fig. 2). The strong beam is used to measure its polarization by means of a polarization measurement which, for simplicity, we assume is *perfect*. For each incoming signal, this device provides Alice with a precise value for the measured angle θ. In this situation, the conditional states emitted by the source can be described as

$$\rho_{\text{out},\theta} = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n_\theta\rangle\langle n_\theta|, \tag{6}$$

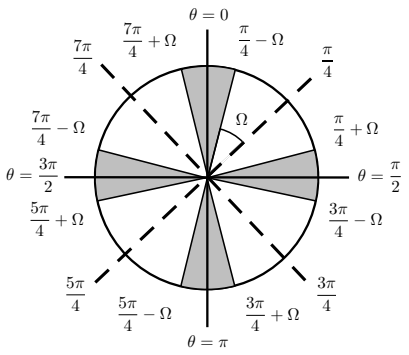

FIG. 3: Graphical representation of the valid regions for the angle θ. These regions are marked in grey. They depend on an acceptance parameter $\Omega \in [0, \pi/4]$.

where θ denotes the value of the angle obtained by Alice's polarization measurement, and μ is given by $\mu = \upsilon t$. In practice, however, as we will show below, it is sufficient if the polarization measurement tells Alice the value of θ within a certain interval.

Whenever $\theta \in \{0, \pi/2, \pi, 3\pi/2\}$ Alice generates one of the four BB84 polarization states perfectly. Note that the creation operators for the polarizations modes in the BB84 protocol, which we shall denote as $b^\dagger_{\text{H}}$, $b^\dagger_{\text{V}}$, $b^\dagger_{\text{L}}$ and $b^\dagger_{\text{R}}$, can be expressed, in terms of the operators $a^\dagger_{\pm 45^\circ}$, as:

$$\begin{aligned}b^\dagger_{\text{H}} &= \frac{1}{\sqrt{2}}\left(a^\dagger_{+45^\circ} + a^\dagger_{-45^\circ}\right),\\ b^\dagger_{\text{V}} &= \frac{1}{\sqrt{2}}\left(a^\dagger_{+45^\circ} - a^\dagger_{-45^\circ}\right),\\ b^\dagger_{\text{L}} &= \frac{1}{\sqrt{2}}\left(a^\dagger_{+45^\circ} + ia^\dagger_{-45^\circ}\right),\\ b^\dagger_{\text{R}} &= \frac{1}{\sqrt{2}}\left(a^\dagger_{+45^\circ} - ia^\dagger_{-45^\circ}\right).\end{aligned} \tag{7}$$

In general, Alice does not need to restrict herself to only those events where she actually prepares a perfect BB84 state, since the probability associated with these ideal events tends to zero. Instead, she can also accept signals with a polarization sufficiently close to the desired ones. This situation is illustrated in Fig. 3, where Alice selects some valid regions for the angle θ. These regions are marked with grey color in the figure. They depend on an acceptance parameter $\Omega \in [0, \pi/4]$ that we optimize. Specifically, whenever the value of θ lies within any of the intervals $\psi \pm (\pi/4 - \Omega)$ with $\psi \in \{0, \pi/2, \pi, 3\pi/2\}$, then Alice considers the pulse emitted by the source as a valid signal. This last condition can also be written as

$$\theta \in \bigcup_{1=0}^{3}\left[(2i+1)\frac{\pi}{4} + \Omega, (2i+3)\frac{\pi}{4} - \Omega\right]. \tag{8}$$

Otherwise, the pulse is discarded afterwards during the post-processing phase of the protocol, and it does not

contribute to the key rate. The probability that a pulse is accepted, $p_{\rm acc}$, is given by

$$p_{\rm acc} = \frac{8\left(\frac{\pi}{4}-\Omega\right)}{2\pi} = 1 - \frac{4\Omega}{\pi}. \tag{9}$$

To increase this probability, one can reduce the value of Ω. Note, however, that this action also results in an increase of the quantum bit error rate (QBER) of the protocol, that we shall denote as E. On the other hand, when Ω increases, we have that both $p_{\rm acc}$ and E decrease. There is a trade-off on the acceptance parameter Ω. A high acceptance probability $p_{\rm acc}$ favors $\Omega \approx 0$, whereas a low QBER favors $\Omega \approx \pi/4$. Note that in the limit where Ω tends to $\pi/4$ we recover the standard BB84 protocol.

A. Lower bound on the secret key rate

The single photon signals emitted by the passive source presented above, averaged over the values of Alice's key bit, are basis-independent. That is, they do not leak any information to Eve about the basis of Alice's signal states. To see this, note that

$$\begin{aligned} &\int_{\frac{7\pi}{4}+\Omega}^{\frac{\pi}{4}-\Omega} |1_\theta\rangle\langle 1_\theta|\, \mathrm{d}\theta + \int_{\frac{3\pi}{4}+\Omega}^{\frac{5\pi}{4}-\Omega} |1_\theta\rangle\langle 1_\theta|\, \mathrm{d}\theta \\ &= \int_{\frac{\pi}{4}+\Omega}^{\frac{3\pi}{4}-\Omega} |1_\theta\rangle\langle 1_\theta|\, \mathrm{d}\theta + \int_{\frac{5\pi}{4}+\Omega}^{\frac{7\pi}{4}-\Omega} |1_\theta\rangle\langle 1_\theta|\, \mathrm{d}\theta \\ &= \frac{(\pi-4\Omega)}{4}\mathbb{1}, \end{aligned} \tag{10}$$

for all $\Omega \in [0, \pi/4]$, and where the single photon state $|1_\theta\rangle$ is given by Eq. (3). Here $\mathbb{1}$ denotes the identity operator in the single photon subspace.

To evaluate the performance of this passive source we use the security analysis provided by Gottesman-Lo-Lütkenhaus-Preskill (GLLP) in Ref. [8]. See also Ref. [16]. It considers that Eve can always obtain full information about the part of the key generated from the multiphoton signals. This pessimistic assumption is also true for the passive transmitter illustrated in Fig. 2 when Alice and Bob use only unidirectional classical communication during the public-discussion phase of the protocol. This result arises from the fact that all the photons contained in a pulse are prepared in the same polarization state and, therefore, no secret key can be distilled with one-way post-processing techniques [17]. Note, however, that such security analysis could leave still room for improvement when Alice and Bob employ two-way classical communication. In this situation, it might be possible to obtain secret key even from the multiphoton pulses since the signal states prepared by the passive device are already mixed at the source. This last scenario, however, is beyond the scope of this paper.

We further assume the typical initial post-processing step in the BB84 protocol, where double click events are not discarded by Bob, but they are randomly assigned to single click events [18, 19]. The secret key rate formula can be written as [8]

$$\begin{aligned} R \;\geq\; & q p_{\rm acc}\Big\{(Q - p_{\rm multi})\big[1 - H(E_1)\big] \\ & - \; Q f(E) H(E)\Big\}. \end{aligned} \tag{11}$$

The parameter q is the efficiency of the protocol ($q = 1/2$ for the standard BB84 protocol, and $q \approx 1$ for its efficient version [20]); Q is the gain, *i.e.*, the probability that Bob obtains a click in his measurement apparatus when Alice sends him a signal state; $f(E)$ is the efficiency of the error correction protocol as a function of the error rate E [21], typically $f(E) \geq 1$ with Shannon limit $f(E) = 1$; $H(x)$ is the binary Shannon entropy function defined as $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$; $p_{\rm multi}$ is the multiphoton probability of the source, *i.e.*,

$$p_{\rm multi} = 1 - e^{-\mu}(1+\mu); \tag{12}$$

and E_1 denotes an upper bound on the single photon error rate. In the case of the standard BB84 protocol without decoy-states, this last quantity is given by [8]

$$E_1 = \frac{E}{1 - \frac{p_{\rm multi}}{Q}}. \tag{13}$$

For simulation purposes we use the channel model and detection device on Bob's side described in Appendix A. This model allows us to calculate the observed experimental parameters Q and E. These quantities are given in Appendix B. Our results, however, can also be applied to any other quantum channel or detection setup, as they depend only on the observed gain and QBER.

The resulting lower bound on the secret key rate is illustrated in Fig. 4 (dashed line). In our simulation we employ the following experimental parameters: the dark count rate of Bob's detectors is $\epsilon_{\rm B} = 1 \times 10^{-6}$, the overall transmittance of his detection apparatus is $\eta_{\rm B} = 0.1$, and the loss coefficient of the quantum channel is $\alpha = 0.2$ dB/km. We further assume that $q = 1/2$, and $f(E) = 1.22$. These data are used as well for the simulations included in Sec. III. With this configuration, it turns out that the optimal value of the mean photon number μ decreases with the distance, while the value of the parameter Ω increases. In particular, μ diminishes from ≈ 0.084 to approximately 4×10^{-3}, while Ω augments from ≈ 0.365 to ≈ 0.76. This result is not surprising. At long distances the gain Q of the protocol is very low and, therefore, it is especially important to keep both the multiphoton probability of the source, and the intrinsic error rate of the signals $\rho_{{\rm out},\theta}$, also low. Fig. 4 includes an inset plot with the optimized parameters μ (dashed line) and Ω (solid line). This figure shows as well a lower bound on the secret key rate for the case of an active source. The cutoff point where the secret key rate drops down to zero is basically the same in both cases. It is given by $l \approx 67.5$ km. This result arises from two main limiting factors: the multiphoton probability

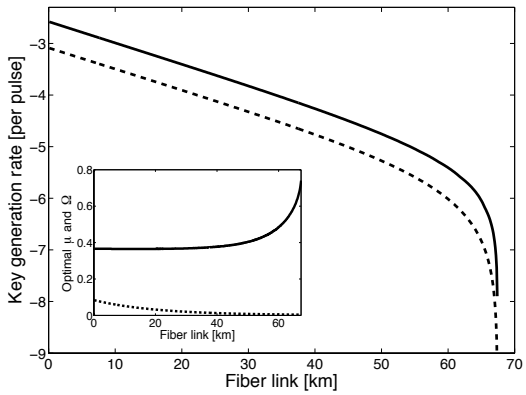

FIG. 4: Lower bound on the secret key rate R given by Eq. (11) in logarithmic scale for the passive source illustrated in Fig. 2 (dashed line). The signal states $\rho_{\mathrm{out},\theta}$ are given by Eq. (6). For simulation purposes, we consider the following experimental parameters: the dark count rate of Bob's detectors is $\epsilon_{\mathrm{B}} = 1 \times 10^{-6}$, the overall transmittance of Bob's detection apparatus is $\eta_{\mathrm{B}} = 0.1$, the loss coefficient of the channel is $\alpha = 0.2$ dB/km, $q = 1/2$, and the efficiency of the error correction protocol is $f(E) = 1.22$. The solid line represents a lower bound on R when Alice employs an active source. The inset figure shows the value for the optimized parameters μ (dashed line) and Ω (solid line) in the passive setup.

of the source, and the dark count rate of Bob's detectors. Note that in these simulations we do not consider any misalignment effect in the channel or in Bob's detection apparatus. From the results shown in Fig. 4 we see that the performance of the passive scheme is similar to the one of an active setup, thus showing the practical interest of the passive source. The (relatively small) difference between the achievable secret key rates in both scenarios is due to two main factors: (a) the probability p_{acc} to accept a pulse emitted by the source, which is $p_{\mathrm{acc}} < 1$ in the passive setup, and $p_{\mathrm{acc}} = 1$ in the active scheme, and (b) the intrinsic error rate of the signals accepted by Alice, that is zero only in the case of an active source.

B. Alternative implementation scheme

The passive setup shown in Fig. 2 requires that Alice employs two independent sources of phase-randomized strong coherent pulses. Alternatively to this scheme, Alice could as well employ, for instance, the device illustrated in Fig. 5. This setup has only one laser diode, but follows a similar spirit like the original scheme shown in Fig. 2, where a polarization measurement is used to determine the polarization of the incoming signals. The main idea is just to replace two single light pulses emitted by two different diodes with two consecutive light pulses generated by only one laser diode.

To keep the analysis simple, the scheme includes as

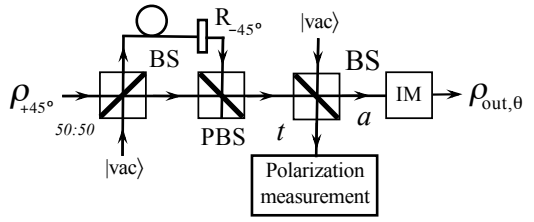

FIG. 5: Alternative implementation scheme with only one pulsed laser source. The delay introduced by one arm of the interferometer is equal to the time difference between two consecutive pulses. The polarization rotator R_{-45° changes the $+45^\circ$ linear polarization of the incoming pulses to -45° linear polarization. The intensity modulator (IM) blocks either all the even or all the odd optical pulses in mode a.

well an intensity modulator (IM) to block either all the even or all the odd pulses in mode a (see Fig. 5). The main reason for blocking half of these pulses is to suppress possible correlations between them. That is, the action of the IM guarantees that the signals that go to Bob are precisely tensor product of states of the form given by Eq. (6). This way we can directly apply the security evaluation provided in the previous section. This transmitter requires, therefore, an active control of the functioning of the IM. Note, however, that this configuration might still be much less of a problem than using a polarization modulator to actively generate BB84 signal states at high rates, since no RNG is needed to control the IM. Thanks to the one-pulse delay introduced by one arm of the interferometer, it can be shown that both setups in Fig. 2 and Fig. 5 are completely equivalent, except from the resulting secret key rate. More precisely, the secret key rate in the passive scheme with two lasers is double than that in the setup illustrated in Fig. 5, since half of the pulses are now discarded.

To conclude, let us mention that similar ideas to the ones presented in this section can also be used in other implementations of the BB84 protocol with a different signal encoding. One example are those QKD experiments based on phase encoding, which turns out to be more suitable to use in combination with optical fibers than polarization encoding [1]. This situation is illustrated in Fig. 6, where now Alice uses a BS of very small transmittance ($t \ll 1$) to split phase-randomized strong coherent pulses into two light beams. The strong beam is used to measure the value of its phase relative to some local reference phase by means of a phase measurement, while Alice sends the weak signal to Bob. Like in the passive source shown in Fig. 2, Alice can select some valid regions for the measured phase, and the analysis presented before also applies straightforwardly to this scenario.

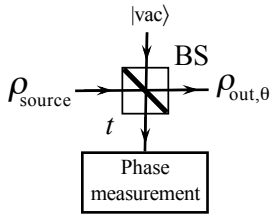

FIG. 6: Basic setup of a passive BB84 QKD phase encoding transmitter with strong coherent light. The mean photon number of the signal states $\rho_{\rm source}$ can be chosen very high; for instance, $\approx 10^8$ photons.

III. PASSIVE TRANSMITTER WITH SINGLE PHOTON SOURCES

The passive state preparation schemes with coherent light introduced in the previous section deliver a key generation rate of order $O(\eta_{\rm sys}^2)$, where $\eta_{\rm sys}$ denotes the overall transmittance of the system. To achieve higher secure key rates over longer distances there are two main alternatives: To combine them with the decoy-state method [9, 10], or to employ SPS. In the first case, Alice can vary the mean photon number of the BB84 signals just by using a variable optical attenuator or a passive decoy-state setup [14]. Here, we will concentrate on the second scenario, and we present a simple passive BB84 source which uses practical SPS. Note that the passive transmitters analyzed in Sec. II cannot be employed with SPS, since those setups need to operate with light pulses of sufficiently high intensity to be able to measure their polarization with certain precision.

The basic setup is illustrated in Fig. 7. It contains four light sources, each of them preparing a different BB84 polarization state. The working principle of this device is rather simple. Let us first consider the ideal case. That is, each photon source in the figure emits precisely one single photon in the desired polarization state, and all detectors have perfect detection efficiency ($\eta_{\rm det} = 1$) and dark count rate $\epsilon_{\rm A}$ equal to zero. In this scenario, we have that whenever Alice observes a click in precisely three of the "signal detectors" $D_{\rm H}$, $D_{\rm V}$, $D_{\rm L}$, and $D_{\rm R}$, and no click in detector D (see Fig. 7), the state generated by the source, that we shall denote as $\rho_{{\rm out},j}$ with $j \in \{{\rm H},{\rm V},{\rm L},{\rm R}\}$, consists of just one photon prepared in the polarization state associated with the signal detector D_j which did not click. For example, suppose that Alice obtains a click in detectors $D_{\rm V}$, $D_{\rm L}$, and $D_{\rm R}$, and no click in detectors $D_{\rm H}$ and D, then the output state is given by $\rho_{\rm out,H} = |1,0\rangle_l\langle 1,0|$, where $|1,0\rangle_l$ denotes a Fock state with one photon in the horizontal polarization mode and zero photons in the vertical polarization mode.

In order to evaluate the performance of this setup in a more realistic scenario, we shall consider practical SPS

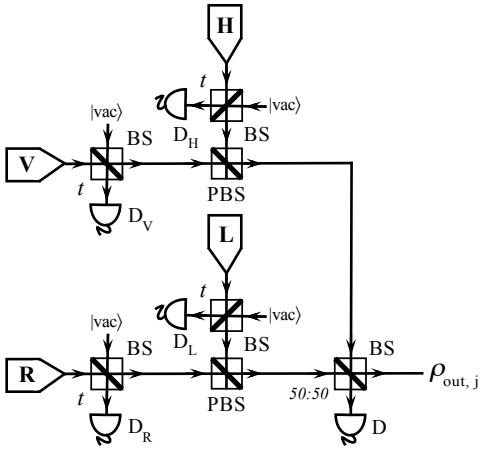

FIG. 7: Basic setup of a passive BB84 QKD transmitter with practical SPS. Each laser diode emits pulses prepared in a different BB84 polarization state: H [horizontal], V [vertical] linear polarizations, and L [left], R [right] circular polarizations. The parameter t represents the transmittance of the BS's. All detectors shown in the figure denote threshold single photon detectors.

emitting Fock diagonal states of the form

$$\rho_{{\rm source},j} = \sum_{n=0}^{\infty} p_n |n\rangle_j\langle n|, \tag{14}$$

with $j \in \{{\rm H},{\rm V},{\rm L},{\rm R}\}$. Furthermore, for simplicity, we assume that the photon number distribution p_n of each source is the same for all them, independently of their polarization.

To characterize the threshold single photon detectors $D_{\rm H}$, $D_{\rm V}$, $D_{\rm L}$, $D_{\rm R}$, and D, we use a POVM with two elements, $F_{\rm vac}$ and $F_{\rm click}$, given by

$$F_{\rm vac} \;=\; (1-\epsilon_{\rm A}) \sum_{n=0}^{\infty} (1-\eta_{\rm det})^n |n\rangle\langle n|, \tag{15}$$

and $F_{\rm click} = \mathbb{1} - F_{\rm vac}$, where again the parameter $\eta_{\rm det}$ denotes the detection efficiency of the detector, and $\epsilon_{\rm A}$ represents its probability of having a dark count. We assume that $\epsilon_{\rm A}$ is, to a good approximation, independent of the incoming signals. The outcome of $F_{\rm vac}$ corresponds to no click in the detector, while the operator $F_{\rm click}$ gives precisely one detection click, which means at least one photon is detected.

After a tedious calculation, one can obtain the conditional output state $\rho_{{\rm out},j}$ given that Alice observes a click only in three of the signal detectors D_i and no click in detectors D and D_j (with $j \neq i$). A mathematical expression for this state, together with its associated probability, is given in Appendix C.

A. Lower bound on the secret key rate

Like in Sec. II A, the single photon signals emitted by the passive source illustrated in Fig. 7 are also basis-independent. To analyze the performance of this source we use again the security results provided by GLLP in Ref. [8]. See also Ref. [16]. The secret key rate formula is given by Eq. (11). Note, however, that such security analysis might overestimate the eavesdropping capabilities of Eve in this scenario even when Alice and Bob use one-way post-processing techniques during the public-discussion phase of the protocol. In contrast to the case analyzed in Sec. II, now multiphoton pulses can contain photons prepared in different polarization states. This effect is similar to the one observed in those EB implementations of the BB84 protocol that use, for instance, a pulsed type-II down conversion source [22]. In this sense, the passive source shown in Fig. 7 might be more robust against the Photon Number Splitting (PNS) attack [23] than an active one, since now Eve might not be able to obtain always full information about the part of the key generated with the multiphoton signals. Still, the multiphoton problem is now on Bob's side who gets a noisy signal, which can contain photons not prepared in Alice's state. The possibility to distill a secret key from multiphoton pulses in this situation constitutes an interesting theoretical question that deserves further investigations, but it is beyond the scope of this paper.

To evaluate the secret key rate formula given by Eq. (11), we need to obtain the gain Q, the error rate E, and the multiphoton probability p_{multi} of the source. These parameters are calculated in Appendix D. For that, we use again the channel model and detection device described in Appendix A. The resulting lower bound on R is illustrated in Figs. 8, 9, and 10, for three different photon number distributions p_n of the practical SPS. For simulation purposes, we use the same experimental data employed in Sec. II A, and we further assume that Alice's detectors have a dark count rate $\epsilon_{\text{A}} = 1 \times 10^{-6}$.

The first example plotted in Fig. 8 considers the case of perfect on-demand SPS, *i.e.*, we impose $p_1 = 1$ in Eq. (14). We study three different situations, depending on the actual value of the efficiency η_{A} of Alice's detectors, and we optimize the transmittance t of the BS's on Alice's side for each case. In particular, we assume $\eta_{\text{A}} = 1$, $\eta_{\text{A}} = 0.5$, and $\eta_{\text{A}} = 0.1$. This figure includes as well a lower bound on R when Alice employs an active source that emits single photon pulses (thick solid line). The cutoff points where the secret key rate drops down to zero are given by $l \approx 201.7$ km (passive source with $\eta_{\text{A}} = 1$), $l \approx 179.3$ km (passive source with $\eta_{\text{A}} = 0.5$), $l \approx 162.5$ km (passive source with $\eta_{\text{A}} = 0.1$), and $l \approx 203$ km (active scheme). From the results shown in this figure we see that, in this ideal scenario where $p_1 = 1$, the performance of the passive scheme is similar to the one of an active setup only when the efficiency of Alice's detectors is relatively high. Note that the difference between the achievable secret key rates in both scenarios comes mainly from the probability $p_{\text{acc}} < 1$ that Alice's transmitter produces a valid signal in the passive scheme (*i.e.*, three of her signals detectors click). Specifically, when the efficiency η_{A} of Alice's detectors is too low, then also the probability p_{acc} decreases significantly, and therefore the secret key rate decreases as well. The value of η_{A} also influences the resulting cutoff points for the secret key rate. For instance, when η_{A} decreases, the intrinsic noise of Alice's signals (*i.e.*, the probability to produce a wrong signal) can increase due to the dark counts of her detectors. Note that this effect becomes more relevant for low η_{A}. As a result, the cutoff point for the secret key rate decreases.

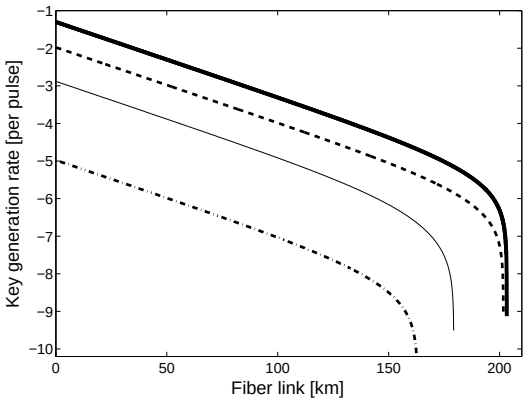

FIG. 8: Lower bound on the secret key rate R given by Eq. (11) in logarithmic scale for the passive setup illustrated in Fig. 7 with perfect on-demand SPS, *i.e.*, $p_1 = 1$ in Eq. (14). In the simulation we consider the following experimental parameters: the dark count rate of Alice's and Bob's detectors is $\epsilon_{\text{A}} = \epsilon_{\text{B}} = 1 \times 10^{-6}$, the overall transmittance of Bob's detection apparatus is $\eta_{\text{B}} = 0.1$, the loss coefficient of the channel is $\alpha = 0.2$ dB/km, $q = 1/2$, and the efficiency of the error correction protocol is $f(E) = 1.22$. We further assume the channel model described in Appendix A, where we neglect any misalignment effect. Otherwise, the actual secure distance will be smaller. The figure includes three cases, depending on the actual value of the efficiency η_{A} of Alice's detectors, and we optimize the transmittance t of the BS's on Alice's side for each case. In particular, we assume $\eta_{\text{A}} = 1$ (dashed line), $\eta_{\text{A}} = 0.5$ (thin solid line), and $\eta_{\text{A}} = 0.1$ (dash-dotted line). The solid line represents a lower bound on R when Alice employs an active source that emits single photon pulses with probability one.

The other two examples illustrated in Figs. 9 and 10 analyze the influence that the vacuum and multiphoton probabilities of the practical SPS can have on the final secret key rate. For that, we consider two different photon number distributions p_n for the SPS described in Eq. (14). In particular, Fig. 9 shows the case where $p_0 = 0.0099$, $p_1 = 0.9882$, and $p_2 = 1 - p_0 - p_1 = 0.0019$, while Fig. 10 assumes $p_0 = 0.2$, $p_1 = 0.785$, and $p_2 = 1 - p_0 - p_1 = 0.015$. In both cases, we evaluate the same three scenarios contemplated in Fig. 8, *i.e.*, we

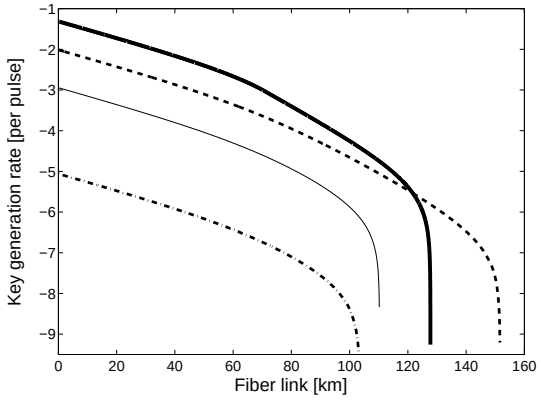

FIG. 9: Lower bound on the secret key rate R given by Eq. (11) in logarithmic scale for the passive setup illustrated in Fig. 7 with imperfect SPS. In particular, we consider that the photon number distribution p_n of the sources is given by $p_0 = 0.0099$, $p_1 = 0.9882$, and $p_2 = 1 - p_0 - p_1 = 0.0019$. We further assume the same experimental data used in Fig. 8. We study three cases, depending on the actual value of the efficiency $\eta_{\rm A}$ of Alice's detectors, and we optimize the transmittance t of the BS's on Alice's side for each case. Specifically, we assume $\eta_{\rm A} = 1$ (dashed line), $\eta_{\rm A} = 0.5$ (thin solid line), and $\eta_{\rm A} = 0.1$ (dash-dotted line). The solid line represents a lower bound on R when Alice employs an active source with photon number distribution p_n in combination with a BS. In this last case, we optimize the value of the transmittance of the BS as a function of the distance.

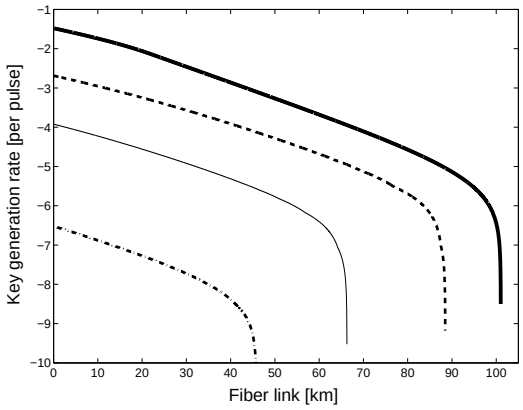

FIG. 10: Lower bound on the secret key rate R given by Eq. (11) in logarithmic scale for the passive setup illustrated in Fig. 7 with imperfect SPS. The photon number distribution p_n of the sources is given by $p_0 = 0.2$, $p_1 = 0.785$, and $p_2 = 1 - p_0 - p_1 = 0.015$. We further assume the same experimental data used in Fig. 8. We study three cases, depending on the actual value of the efficiency $\eta_{\rm A}$ of Alice's detectors, and we optimize the transmittance t of the BS's on Alice's side for each case. In particular, we assume $\eta_{\rm A} = 1$ (dashed line), $\eta_{\rm A} = 0.5$ (thin solid line), and $\eta_{\rm A} = 0.1$ (dash-dotted line). The solid line represents a lower bound on R when Alice employs an active source with photon number distribution p_n in combination with a BS. In this last case, we optimize the value of the transmittance of the BS as a function of the distance.

consider $\eta_{\rm A} = 1$, $\eta_{\rm A} = 0.5$, and $\eta_{\rm A} = 0.1$. As expected, when the vacuum probability p_0 augments, the probability $p_{\rm acc}$ decreases and, therefore, the secret key rate decreases as well. Similarly, if the multiphoton probability p_2 increases, the intrinsic noise of Alice's signals also augments, and both the secret key rate and its cutoff point decreases. For comparison purposes, we consider as well the situation where Alice uses an active source (thick solid line) in combination with a BS whose transmittance is optimized with the distance. In this last case, the slope of the lower bound on R (when Alice employs an active setup) increases slightly when the transmittance of this additional BS starts to be less than one. This occurs, respectively, at $l \approx 71$ km (see Fig. 9), and $l \approx 22$ km (see Fig. 10). From these results, we see that also in these two examples the performance of the passive scheme is comparable to the one of an active setup when $\eta_{\rm A}$ is sufficiently high. Furthermore, it is interesting to note that the distance covered by a passive transmitter might be even longer than the one of an active configuration for some values of the photon number distribution p_n and of the parameter $\eta_{\rm A}$ (see, for instance, the dashed line in Fig. 9). Let us emphasize, moreover, that, as discussed above, in our security analysis we assume that multiphoton signals are always insecure (which is actually true only in the case of an active device), and, therefore, there might be still further room for improvement in the secret key rate which can be achieved with a passive device.

The passive source shown in Fig. 7 might be an interesting alternative to implement the BB84 QKD protocol with practical SPS. However, let us mention that to date there are still two main experimental challenges that need to be overcomed in order to obtain relevant secret key rates with such a device. On the one hand, we need to develop single photon detectors with high quantum efficiency that can operate at high clock rate. This represents an interesting technological challenge, especially at telecom wavelengths where the efficiency of present-day single photon detectors lie typically at roughly 10-15%. In recent years, however, this field has advanced substantially and there are reasons to be optimistic; for instance, it has been shown lately that superconducting transition-edge sensor detectors can provide photon number resolving capabilities at telecom wavelengths with 95% efficiency and negligible noise [24]. At visible wavelengths, silicon avalanche photodiodes (APD) are already commercially available to offer high quantum efficiencies (up to about 70-80%) and low dark count rates. This last scenario, for example, is particularly relevant for free-space QKD. On the other hand, we need to design high-quality on-demand SPS. Note that the photon number statistics used for simulations purposes in this section assume on-demand SPS that are still beyond our present experimental capability [25]. For instance, the normal-

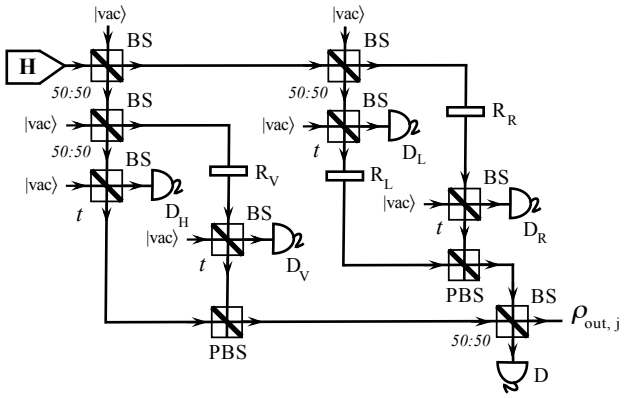

FIG. 11: Alternative implementation scheme with only one photon source. The polarization rotators $R_{\rm V}$, $R_{\rm L}$, and $R_{\rm R}$, change the horizontal polarization of the incoming pulses to vertical polarization, left circular polarization, and right circular polarization, respectively.

ized second-order correlation function $g^{(2)}$ and average photon number per pulse $\bar{n}$ of the sources used in Figs. 9 and 10 are, respectively, $g^{(2)} = 0.0039$ and $\bar{n} = 0.992$, and $g^{(2)} = 0.0452$ and $\bar{n} = 0.815$. Despite the remarkable progress that has been made in recent years to generate indistinguishable on demand single photons, nowadays sub-Poissonian sources have a normalized second-order correlation function that lies typically between 0.05 and 0.2 [25]. However, the biggest experimental challenge here is to increase the achievable collection efficiency, which is usually below 10%. This means that the probability to obtain an empty pulse is still rather high, and therefore $\bar{n}$ is relatively small [25]. As a result, the acceptance probability $p_{\rm acc}$ of the passive BB84 source shown in Fig. 7 would be also quite small. Alternatively, one may use heralded SPS based on a parametric down conversion process, where the emission of an individual photon is heralded by the detection of the twin-photon [26]. For instance, the photon number distributions of the sources used above can be generated with this type of sources. In this last case, however, the secret key rate formula should include an additional factor accounting for this detection probability. As a consequence, the final key rate can be substantially reduced.

To conclude this section, let as mention that (as in Sec. II B) instead of using the passive source illustrated in Fig. 7, Alice could as well employ, for instance, the alternative scheme illustrated in Fig. 11. This setup is similar to the one shown in Fig. 7, but has only one photon source, which might make it more robust against side-channel attacks hidden in the imperfections of the light sources. The main idea is to replace four single-photon pulses (with different polarizations) emitted by four SPS by one four-photon pulse (with all their photons prepared in the same polarization state) together with polarization rotators. The argumentation here goes similar to the passive device presented in Fig. 7, and we omit it for simplicity. The resulting secret key rate in this scenario, however, might be lower than that in the passive setup analyzed in Sec. III, since now the probability $p_{\rm acc}$ to consider an output pulse as valid is also lower. Note that the passive scheme shown in Fig. 11 has the additional requirement that each photon of a four-photon pulse needs to follow a different optical path, which is selected by means of 50 : 50 BS's. The photon number statistics of the output signals generated by both passive schemes are also different.

IV. CONCLUSION

Typical experimental realizations of quantum key distribution (QKD) protocols prepare the signal states by means of an active source. In this article, we have investigated two different methods to passively generate the signal states of the Bennett-Brassard 1984 (BB84) QKD protocol. Our methods need only linear optical components and photodetectors, and represent an alternative to those active sources that use external-driven elements.

In particular, we have showed that both coherent light and practical single photon sources are suitable for passive generation of BB84 signals. In the asymptotic limit of an infinite long experiment, we have proved that the secret key rate delivered by a passive source with coherent light is similar to the one provided by an active source, thus showing the practical interest of the passive scheme. When Alice uses practical single photon sources, we have showed that the distance covered by a passive transmitter might be longer than the one of an active configuration. This result is caused by the capacity of the passive scheme to reduce the number of multiphoton emissions of the source via a post-selection mechanism.

The main focus of this paper has been polarization-based realizations of the BB84 protocol, which are particularly relevant for free-space QKD. However, we have also showed that similar ideas can as well be applied to other practical scenarios with different signal encodings, like, for instance, those QKD experiments based on phase encoding, which are more suitable to use in combination with optical fibers.

V. ACKNOWLEDGEMENTS

The authors thank R. Kaltenbaek and B. Qi for very useful discussions. M. C. especially thanks the Institute for Quantum Computing (University of Waterloo) and the University of Toronto for hospitality and support during his stay in both institutions. This work was supported by CFI, CIPI, the CRC program, CIFAR, MITACS, NSERC, OIT, QuantumWorks, and by Xunta de Galicia (Spain, grant INCITE08PXIB322257PR).

Appendix A: Bob's detection setup and channel model

In this Appendix we include a simple model to characterize Bob's detection device and the behavior of the quantum channel. This model is used in Sec. II and Sec. III to evaluate the performance of the two passive BB84 state preparation schemes that we present there.

For simplicity, in our calculations we shall consider that Bob employs an active BB84 detection setup. Note, however, that the results contained in Sec. II and Sec. III can be straightforwardly adapted to cover as well the case where Bob uses a detection apparatus with passive basis choice [12].

Specifically, we assume that Bob's detection scheme consists of a polarization analyzer and a polarization shifter which effectively changes the polarization basis of the subsequent measurement. The polarization analyzer has two detectors, each of them monitoring the output of a PBS. These detectors are characterized by their detection efficiency $\eta_{\rm det}$ and their dark count rate $\epsilon_{\rm B}$ [27]. Furthermore, we suppose that both detectors are equal, and cannot distinguish the number of photons of arrival signals. They provide only two possible outcomes: "click" (at least one photon is detected), and "no click" (no photon is detected in the pulse).

The action of such detection device can be described by two positive operator value measures (POVM), one for each of the two BB84 polarization bases $\beta \in \{l, c\}$, where l denotes a linear polarization basis and c is a circular polarization basis [28]. Each POVM contains four elements: $G^\beta_{\rm vac}$, G^β_0, G^β_1, and $G^\beta_{\rm dc}$. The outcome of the first operator, $G^\beta_{\rm vac}$, corresponds to no click in the detectors, the following two POVM operators, G^β_0 and G^β_1, give precisely one detection click (these are the desired measurements), and the last one, $G^\beta_{\rm dc}$, gives rise to both detectors being triggered. These operators can be written as

$$\begin{aligned} G^\beta_{\rm vac} &= [1-\epsilon_{\rm B}(2-\epsilon_{\rm B})]F^\beta_{\rm vac}, \\ G^\beta_0 &= (1-\epsilon_{\rm B})\epsilon_{\rm B}F^\beta_{\rm vac} + (1-\epsilon_{\rm B})F^\beta_0, \\ G^\beta_1 &= (1-\epsilon_{\rm B})\epsilon_{\rm B}F^\beta_{\rm vac} + (1-\epsilon_{\rm B})F^\beta_1, \\ G^\beta_{\rm dc} &= \mathbb{1} - G^\beta_{\rm vac} - G^\beta_0 - G^\beta_1, \end{aligned} \tag{A1}$$

where the operators $F^\beta_{\rm vac}$, F^β_0, F^β_1, and $F^\beta_{\rm dc}$ are defined below. Eq. (A1) assumes that the background rate, is, to a good approximation, independent of the signal detection. Moreover, for easiness of notation, we only consider a background contribution coming from dark counts of Bob's detectors and we neglect other background contributions like, for instance, stray light arising from timing pulses which are not completely filtered out in reception.

The definition of the operators $F^\beta_{\rm vac}$, F^β_0, F^β_1, and $F^\beta_{\rm dc}$ includes as well the effect of the quantum channel. These operators characterize Bob's detection device, together with the action of the quantum channel, in the case of noiseless detectors. We consider a simple model of a quantum channel in the absence of eavesdropping; it just consists of a BS of transmittance $\eta_{\rm channel}$. For simplicity, here we neglect any misalignment effect in the channel. In this scenario, the operators $F^\beta_{\rm vac}$, F^β_0, F^β_1, and $F^\beta_{\rm dc}$ have the form [18, 29]

$$\begin{aligned} F^\beta_{\rm vac} &= \sum_{n,m=0}^{\infty} (1-\eta_{\rm sys})^{n+m} |n,m\rangle_\beta\langle n,m|, \\ F^\beta_0 &= \sum_{n,m=0}^{\infty} [1-(1-\eta_{\rm sys})^n](1-\eta_{\rm sys})^m |n,m\rangle_\beta\langle n,m|, \\ F^\beta_1 &= \sum_{n,m=0}^{\infty} [1-(1-\eta_{\rm sys})^m](1-\eta_{\rm sys})^n |n,m\rangle_\beta\langle n,m|, \\ F^\beta_{\rm dc} &= \sum_{n,m=0}^{\infty} [1-(1-\eta_{\rm sys})^n][1-(1-\eta_{\rm sys})^m] \\ &\quad \times |n,m\rangle_\beta\langle n,m|, \end{aligned} \tag{A2}$$

with $\beta \in \{l, c\}$. The signals $|n,m\rangle_l$ ($|n,m\rangle_c$) represent the state which has n photons in the horizontal (circular left) polarization mode and m photons in the vertical (circular right) polarization mode. The parameter $\eta_{\rm sys}$ denotes the overall transmittance of the system. This quantity can be written as

$$\eta_{\rm sys} = \eta_{\rm channel}\eta_{\rm B}, \tag{A3}$$

where $\eta_{\rm B}$ denotes the overall transmittance of Bob's detection apparatus, *i.e.*, $\eta_{\rm B}$ includes the transmittance of any optical component within Bob's measurement device together with the efficiency $\eta_{\rm det}$ of his detectors.

The parameter $\eta_{\rm channel}$ can be related with a transmission distance d measured in km for the given QKD scheme as

$$\eta_{\rm channel} = 10^{-\frac{\alpha d}{10}}, \tag{A4}$$

where α represents the loss coefficient of the channel (*e.g.*, free-space, or an optical fiber) measured in dB/km.

Appendix B: Gain and QBER of a passive BB84 QKD setup with coherent light

In this Appendix, we calculate the observed gain Q and error rate E for the passive QKD device introduced in Sec. II. For that, we use the channel model and detection apparatus described in Appendix A. In the scenario considered, it turns out that the gain is independent of the actual polarization of the signals $\rho_{{\rm out},\theta}$ given by Eq. (6) and the basis β used to measure them. This parameter has the form

$$Q = 1 - {\rm Tr}(G^\beta_{\rm vac}\rho_{{\rm out},\theta}) = 1 - (1-\epsilon_{\rm B})^2 e^{-\mu\eta_{\rm sys}}, \tag{B1}$$

for all θ and β.

The calculation of E is slightly more involved, since the error rate varies depending on the value of the angle θ. By symmetry, however, we can restrict ourselves to investigate the QBER in only one of the valid regions illustrated in Fig. 3; note that the error rate is the same in all of them. For instance, let us consider the case where $\theta \in [7\pi/4+\Omega, \pi/4-\Omega]$ (which corresponds to the horizontal polarization interval), and let E_θ denote the error rate of a signal state $\rho_{\text{out},\theta}$ in that region. This quantity can be written as

$$E_\theta = \text{Tr}(G_1^l \rho_{\text{out},\theta}) + \frac{1}{2}\text{Tr}(G_{\text{dc}}^l \rho_{\text{out},\theta}). \tag{B2}$$

The first term in the summation represents the probability that the signal hits the wrong detector on Bob's side, *i.e.*, he observes a click in the detector associated with vertical polarization. The second term in Eq. (B2) is the probability to have a double click on his detection apparatus and assign to it a single click in the wrong detector. Using Eqs. (A1)-(A2), we have that E_θ can be further simplified as

$$\begin{aligned} E_\theta &= \frac{1}{2Q}\Big\{\epsilon_{\text{B}}(\epsilon_{\text{B}}-1)f_{0,\theta} + \big[2+\epsilon_{\text{B}}(\epsilon_{\text{B}}-3)\big]f_{1,\theta} \\ &+ \big[1+\epsilon_{\text{B}}(\epsilon_{\text{B}}-2)\big]f_{\text{dc},\theta} + \epsilon_{\text{B}}(2-\epsilon_{\text{B}})\Big\}, \end{aligned} \tag{B3}$$

where

$$f_{i,\theta} = \text{Tr}(F_i^l \rho_{\text{out},\theta}), \tag{B4}$$

for all $i \in \{0, 1, \text{dc}\}$, and $\theta \in [7\pi/4+\Omega, \pi/4-\Omega]$. In order to calculate the probabilities $f_{i,\theta}$ we use Eqs. (3)-(7) to first rewrite the state $\rho_{\text{out},\theta}$ given by Eq. (6) as

$$\begin{aligned} \rho_{\text{out},\theta} &= e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}\frac{1}{4^n}\sum_{k,k'=0}^{n}\sqrt{\binom{n}{k}\binom{n}{k'}} \\ &\times \left(1+e^{i\theta}\right)^k\left(1+e^{-i\theta}\right)^{k'}\left(1-e^{i\theta}\right)^{n-k} \\ &\times \left(1-e^{-i\theta}\right)^{n-k'}|k, n-k\rangle_l\langle k', n-k'|, \end{aligned} \tag{B5}$$

where $|n,m\rangle_l$ represents again the state which has n photons in the horizontal polarization mode and m in the vertical polarization mode. We obtain

$$\begin{aligned} f_{0,\theta} &= e^{-\eta_{\text{sys}}\mu}\Big[-1+e^{\frac{1}{2}\eta_{\text{sys}}\mu(1+\cos\theta)}\Big], \\ f_{1,\theta} &= e^{-\eta_{\text{sys}}\mu}\Big[-1+e^{\frac{1}{2}\eta_{\text{sys}}\mu(1-\cos\theta)}\Big], \end{aligned} \tag{B6}$$

and

$$\begin{aligned} f_{\text{dc},\theta} &= 1+e^{-\eta_{\text{sys}}\mu}-e^{-\frac{1}{2}\eta_{\text{sys}}\mu(1+\cos\theta)} \\ &\quad -e^{-\eta_{\text{sys}}\mu\sin^2\left(\frac{\theta}{2}\right)}. \end{aligned} \tag{B7}$$

The quantum bit error rate E is then given by

$$E = \frac{2}{\pi-4\Omega}\int_{\frac{7\pi}{4}+\Omega}^{\frac{\pi}{4}-\Omega} E_\theta \, \text{d}\theta, \tag{B8}$$

and we solve this equation numerically.

Appendix C: Conditional output state

In this Appendix we provide a mathematical expression for the conditional output state $\rho_{\text{out},j}$ introduced in Sec. III together with its associated probability. This signal can be written as

$$\rho_{\text{out},j} = \frac{1}{N}\sum_{n,m,k,l=0}^{\infty} q_{(n,m,k,l)}\sigma_j^{n,m,k,l}, \tag{C1}$$

where the parameters $q_{(n,m,k,l)}$ are given by $q_{(n,m,k,l)} = u_n q_m q_k q_l$, with

$$\begin{aligned} u_n &= (1-\epsilon_{\text{A}})t^n\sum_{k=n}^{\infty}p_k\binom{k}{k-n}\Big[(1-\eta_{\text{det}}) \\ &\times (1-t)\Big]^{k-n}, \end{aligned} \tag{C2}$$

and

$$\begin{aligned} q_n &= t^n\sum_{k=n}^{\infty}p_k\binom{k}{k-n}(1-t)^{k-n}\Big[1-(1-\epsilon_{\text{A}}) \\ &\times (1-\eta_{\text{det}})^{k-n}\Big]. \end{aligned} \tag{C3}$$

The states $\sigma_j^{n,m,k,l}$ have the form

$$\begin{aligned} \sigma_j^{n,m,k,l} &= (1-\epsilon_{\text{A}})\frac{2^{-(n+m)}4^{-(k+l)}}{n!m!k!l!}\sum_{w,w'=0}^{k+l}\sum_{r=0}^{\min\{w+n,w'+n\}}\sum_{s=0}^{\min\{k+l+m-w,k+l+m-w'\}} g_{(n,m,k,l,w,w',r,s)}(1-\eta_{\text{det}})^{r+s} \\ &\times h_{(n,m,k,l,w,w',r,s)}|w+n-r, k+l+m-w-s\rangle_j\langle w'+n-r, k+l+m-w'-s|, \end{aligned} \tag{C4}$$

where $|n,m\rangle_j$ represents the state which has n photons in the polarization mode associated with the signal detector D_j which did not click, and m photons in its orthogonal polarization mode. The functions $g_{(n,m,k,l,w,w',r,s)}$ and $h_{(n,m,k,l,w,w',r,s)}$ which appear in Eq. (C4) are defined, respectively, as

$$\begin{aligned} g_{(n,m,k,l,w,w',r,s)} &= f_{(w,k,l)} f_{(w',k,l)} f_{(r,w,n)} f_{(r,w',n)} \\ &\times f_{(s,k+l-w,m)} f_{(s,k+l-w',m)}, \end{aligned} \quad \text{(C5)}$$

with $f_{(x,y,z)}$ given by

$$f_{(x,y,z)} = \sum_{s=\max\{0,x-z\}}^{\min\{x,y\}} \binom{y}{s}\binom{z}{x-s}(-1)^{z-x+s}, \quad \text{(C6)}$$

and

$$\begin{aligned} h_{(n,m,k,l,w,w',r,s)} &= r!s!\sqrt{(w+n-r)!}\sqrt{(w'+n-r)!} \\ &\times\sqrt{(k+l+m-w-s)!}\sqrt{(k+l+m-w'-s)!}. \end{aligned} \quad \text{(C7)}$$

The normalization factor N of the output states $\rho_{\text{out},j}$ does not depend on the parameter j. It can be calculated as

$$N = \sum_{n,m,k,l=0}^{\infty} q_{(n,m,k,l)} \text{Tr}(\sigma_j^{n,m,k,l}), \quad \text{(C8)}$$

where the quantities $\text{Tr}(\sigma_j^{n,m,k,l})$ are given by

$$\begin{aligned} \text{Tr}(\sigma_j^{n,m,k,l}) &= (1-\epsilon_{\text{A}}) \frac{2^{-(n+m)}4^{-(k+l)}}{n!m!k!l!} \sum_{w=0}^{k+l}\sum_{r=0}^{w+n} \\ &\sum_{s=0}^{k+l+m-w} (1-\eta_{\text{det}})^{r+s} g_{(n,m,k,l,w,w,r,s)} \\ &\times\ h_{(n,m,k,l,w,w,r,s)}. \end{aligned} \quad \text{(C9)}$$

for all j.

Finally, we have that the probability that Alice produces a valid output state, *i.e.*, only three of her signal detectors D_i click and D does not click, that we shall denote as p_{acc}, is given by

$$p_{\text{acc}} = 4N. \quad \text{(C10)}$$

Appendix D: Gain, QBER, and multiphoton probability of a passive BB84 QKD setup with practical SPS

It turns out that the gain of the protocol is independent of the polarization j of the signals $\rho_{\text{out},j}$ and the basis β used to measure them. This parameter can be expressed as

$$\begin{aligned} Q &= 1 - \text{Tr}(G_{\text{vac}}^{\beta}\rho_{\text{out},j}) = 1 - \frac{[1-\epsilon_{\text{B}}(2-\epsilon_{\text{B}})](1-\epsilon_{\text{A}})}{N} \\ &\times \sum_{n,m,k,l=0}^{\infty} q_{(n,m,k,l)} \frac{2^{-(n+m)}4^{-(k+l)}}{n!m!k!l!} \sum_{w=0}^{k+l}\sum_{r=0}^{w+n} \\ &\times \sum_{s=0}^{k+l+m-w} (1-\eta_{\text{det}})^{r+s}(1-\eta_{\text{sys}})^{n+m+k+l-r-s} \\ &\times\ g_{(n,m,k,l,w,w,r,s)} h_{(n,m,k,l,w,w,r,s)}, \end{aligned} \quad \text{(D1)}$$

for all j and β.

The QBER has also the same value for all possible polarization states $\rho_{\text{out},j}$ emitted by Alice. Therefore, like in Appendix B, in order to calculate it we can restrict ourselves to only one given polarization j. For instance, let us assume that the state produced by the source is $\rho_{\text{out,H}}$, that is, $j = \text{H}$. In this case, the error rate can be written as

$$E = \text{Tr}(G_1^l \rho_{\text{out,H}}) + \frac{1}{2}\text{Tr}(G_{\text{dc}}^l \rho_{\text{out,H}}), \quad \text{(D2)}$$

where the first term is the probability that the signal hits the wrong detector on Bob's side, and the second term denotes the probability to have a double click and assign to it a single click in the wrong detector. Like in Appendix B, this quantity can be further simplified as

$$\begin{aligned} E &= \frac{1}{2Q}\Big\{\epsilon_{\text{B}}(\epsilon_{\text{B}}-1) f_{0,\text{H}} + \big[2+\epsilon_{\text{B}}(\epsilon_{\text{B}}-3)\big] f_{1,\text{H}} \\ &+ \big[1+\epsilon_{\text{B}}(\epsilon_{\text{B}}-2)\big] f_{\text{dc,H}} + \epsilon_{\text{B}}(2-\epsilon_{\text{B}})\Big\}, \end{aligned} \quad \text{(D3)}$$

where $f_{i,\text{H}} = \text{Tr}(F_i^l \rho_{\text{out,H}})$ for all $i \in \{0,1,\text{dc}\}$. The probabilities $f_{i,\text{H}}$ can be obtained directly using Eqs. (A2)-(C1). In particular, we find that

$$\begin{aligned} f_{0,\text{H}} &= \frac{(1-\epsilon_{\text{A}})}{N} \sum_{n,m,k,l=0}^{\infty} q_{(n,m,k,l)} \frac{2^{-(n+m)}4^{-(k+l)}}{n!m!k!l!} \\ &\times \sum_{w=0}^{k+l}\sum_{r=0}^{w+n}\sum_{s=0}^{k+l+m-w} (1-\eta_{\text{det}})^{r+s} \\ &\times\ [1-(1-\eta_{\text{sys}})^{w+n-r}](1-\eta_{\text{sys}})^{k+l+m-w-s} \\ &\times\ g_{(n,m,k,l,w,w,r,s)} h_{(n,m,k,l,w,w,r,s)}, \\ f_{1,\text{H}} &= \frac{(1-\epsilon_{\text{A}})}{N} \sum_{n,m,k,l=0}^{\infty} q_{(n,m,k,l)} \frac{2^{-(n+m)}4^{-(k+l)}}{n!m!k!l!} \\ &\times \sum_{w=0}^{k+l}\sum_{r=0}^{w+n}\sum_{s=0}^{k+l+m-w} (1-\eta_{\text{det}})^{r+s}(1-\eta_{\text{sys}})^{w+n-r} \\ &\times\ [1-(1-\eta_{\text{sys}})^{k+l+m-w-s}] g_{(n,m,k,l,w,w,r,s)} \\ &\times\ h_{(n,m,k,l,w,w,r,s)}, \end{aligned} \quad \text{(D4)}$$

and

$$f_{\mathrm{dc,H}} = \frac{(1-\epsilon_{\mathrm{A}})}{N}\sum_{n,m,k,l=0}^{\infty} q_{(n,m,k,l)}\frac{2^{-(n+m)}4^{-(k+l)}}{n!m!k!l!} \times \sum_{w=0}^{k+l}\sum_{r=0}^{w+n}\sum_{s=0}^{k+l+m-w}(1-\eta_{\mathrm{det}})^{r+s} \times [1-(1-\eta_{\mathrm{sys}})^{w+n-r}][1-(1-\eta_{\mathrm{sys}})^{k+l+m-w-s}] \times g_{(n,m,k,l,w,w,r,s)}h_{(n,m,k,l,w,w,r,s)}. \quad \text{(D5)}$$

Finally, the multiphoton probability of the source, p_{multi}, is as well independent of the value of the polarization j. It can be obtained as

$$p_{\mathrm{multi}} = 1-\sum_{n=0}^{1}\sum_{m=0}^{1-n}\mathrm{Tr}\Big(|n,m\rangle_j\langle n,m|\rho_{\mathrm{out},j}\Big) = 1-p_{0,0,j}-p_{0,1,j}-p_{1,0,j}, \quad \text{(D6)}$$

where the probabilities $p_{n,m,j}$ are defined as

$$p_{n,m,j} \equiv \langle n,m|\rho_{\mathrm{out},j}|n,m\rangle_j. \quad \text{(D7)}$$

After a short calculation, we find that

$$p_{0,0,j} = \frac{1}{N}\sum_{n,m,k,l=0}^{\infty} q_{(n,m,k,l)}\frac{2^{-(n+m)}4^{-(k+l)}}{n!m!k!l!} \times (1-\epsilon_{\mathrm{A}})\sum_{w=0}^{k+l}(1-\eta_{\mathrm{det}})^{n+m+k+l} \times g_{(n,m,k,l,w,w,w+n,k+l+m-w)} \times h_{(n,m,k,l,w,w,w+n,k+l+m-w)}, \quad \text{(D8)}$$

$$p_{0,1,j} = \frac{1}{N}\sum_{n,m,k,l=0}^{\infty} q_{(n,m,k,l)}\frac{2^{-(n+m)}4^{-(k+l)}}{n!m!k!l!} \times \sum_{w=0}^{\min\{k+l,k+l+m-1\}}(1-\eta_{\mathrm{det}})^{n+m+k+l-1} \times (1-\epsilon_{\mathrm{A}})g_{(n,m,k,l,w,w,w+n,k+l+m-w-1)} \times h_{(n,m,k,l,w,w,w+n,k+l+m-w-1)}, \quad \text{(D9)}$$

and

$$p_{1,0,j} = \frac{1}{N}\sum_{n,m,k,l=0}^{\infty} q_{(n,m,k,l)}\frac{2^{-(n+m)}4^{-(k+l)}}{n!m!k!l!} \times \sum_{w=\max\{0,1-n\}}^{k+l}(1-\eta_{\mathrm{det}})^{n+m+k+l-1} \times (1-\epsilon_{\mathrm{A}})g_{(n,m,k,l,w,w,w+n-1,k+l+m-w)} \times h_{(n,m,k,l,w,w,w+n-1,k+l+m-w)}. \quad \text{(D10)}$$

[1] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); M. Dušek, N. Lütkenhaus and M. Hendrych, Progress in Optics **49**, Edt. E. Wolf (Elsevier), 381 (2006); V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] G. S. Vernam, J. Am. Inst. Electr. Eng. **XLV**, 109 (1926).

[3] C. H. Bennett and G. Brassard, Proc. IEEE Int. Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE Press, New York, 175 (1984).

[4] R. J. Hughes, J. E. Nordholt, D. Derkacs and C. G. Peterson, New J. Phys. **4**, 43 (2002); C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity, Nature **419**, 450 (2002).

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, J. Cryptology **5**, 3 (1992); A. Muller, J. Bréguet and N. Gisin, Europhysics Lett. **23**, 383 (1993); J. Bréguet, A. Muller and N. Gisin, J. Mod. Opt. **41**, 2405 (1994); A. Muller, H. Zbinden and N. Gisin, Nature **378**, 449 (1995); A. Muller, H. Zbinden and N. Gisin, Europhysics Lett. **33**, 335 (1996); P. Townsend, IEEE Photonics Tech. Lett. **10**, 1048 (1998); G. B. Xavier, N. Walenta, G. Vilela de Faria, G. P. Temporão, N. Gisin, H. Zbinden and J. P. von der Weid, New J. Phys. **11**, 045015 (2009).

[6] N. Lütkenhaus, Appl. Phys. B: Lasers Opt. **69**, 395 (1999); D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003); X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki and H.-K. Lo, Phys. Rev. A **74**, 032330 (2006); V. Scarani, A. Acín, G. Ribordy and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004); B. Kraus, N. Gisin and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005); R. Renner, N. Gisin and B. Kraus, Phys. Rev. A **72**, 012332 (2005); J. M. Renes and Graeme Smith, Phys. Rev. Lett. **98**, 020502 (2007).

[7] H. Inamori, N. Lütkenhaus and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[8] D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[9] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); X.-B. Wang, Phys. Rev. A **72**, 012322 (2005); X.-B. Wang, Phys. Rev. A **72**, 049908(E) (2005).

[10] Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006); Y. Zhao, B. Qi, X. Ma,

H.-K. Lo and L. Qian, Proc. of IEEE International Symposium on Information Theory (ISIT'06), 2094 (2006); 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); 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); 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); Z. L. Yuan, A. W. Sharpe and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007); Z.-Q. Yin, Z.-F. Han, W. Chen, F.-X. Xu, Q.-L. Wu and G.-C. Guo, Chin. Phys. Lett **25**, 3547 (2008); J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka and A. Tomita, Preprint quant-ph/0705.3081; J. F. Dynes, Z. L. Yuan, A. W. Sharpe and A. J. Shields, Optics Express **15**, 8465 (2007).

[11] J. F. Dynes, Z. L. Yuan, A. W. Sharpe and A. J. Shields, Appl. Phys. Lett. **93**, 1 (2008); B. Qi, Y.-M. Chi, H.-K. Lo and L. Qian, Opt. Lett. **35**, 312 (2010); K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama and P. Davis, Opt. Express **18**, 5512 (2010); M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer and H. Weinfurter, Opt. Express **18**, 13029 (2010).

[12] J. G. Rarity, P. C. M. Owens and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).

[13] W. Mauerer and C. Silberhorn, Phys. Rev. A **75**, 050305(R) (2007); Y. Adachi, T. Yamamoto, M. Koashi and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007); X. Ma and H.-K. Lo, New J. Phys. **10**, 073018 (2008).

[14] M. Curty, T. Moroder, X. Ma and N. Lütkenhaus, Opt. Lett. **34**, 3238 (2009); Y. Adachi, T. Yamamoto, M. Koashi and N. Imoto, New J. Phys. **11**, 113033 (2009); M. Curty, X. Ma, B. Qi and T. Moroder, Phys. Rev. A **81**, 022310 (2010).

[15] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin and H. Zbinden, Phys. Rev. A **63**, 012309 (2000); W. Tittel, J. Brendel, H. Zbinden and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).

[16] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[17] T. Moroder, M. Curty and N. Lütkenhaus, Phys. Rev. A **74**, 052301 (2006).

[18] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).

[19] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008); N. J. Beaudry, T. Moroder and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[20] H.-K. Lo, H. F. C. Chau and M. Ardehali, J. Cryptology **18**, 133 (2005).

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

[22] P. Kok and S. L. Braunstein, Phys. Rev. A **61**, 042304 (2000).

[23] B. Huttner, N. Imoto, N. Gisin and T. Mor, Phys. Rev. A **51**, 1863 (1995); G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[24] A. E. Lita, A. J. Miller and S. W. Nam, Opt. Express **16**, 3032 (2008).

[25] B. Lounis and M. Orrit, Rep. Prog. Phys. **68**, 1129 (2005); A. J. Shields, Nature Phot. **1**, 215 (2007); D. J. P. Ellis, A. J. Bennett, A. J. Shields, P. Atkinson and D. A. Ritchie, Appl. Phys. Lett. **90**, 233514 (2007); M. Hijlkema, B. Weber, H. P. Specht, S. C. Webster, A. Kuhn and G. Rempe, Nature Phys. **3**, 253 (2007). J. Bochmann, M. Mücke, G. Langfahl-Klabes, C. Erbel, B. Weber, H. P. Specht, D. L. Moehring and G. Rempe, Phys. Rev. Lett. **101**, 223601 (2008); D. A. Simpson, E. Ampem-Lassen, B. C. Gibson, S. Trpkovski, F. M. Hossain, S. T. Huntington, A. D. Greentree, L. C. L. Hollenberg and S. Prawer, Appl. Phys. Lett. **94**, 203107 (2009); E. B. Flagg, A. Muller, J. W. Robertson, S. Fouta, D. G. Deppe, M. Xiao, W. Ma, G. J. Salamo and C. K. Shih, Nature Phys. **5**, 203 (2009); D. Englund, B. Shields, K. Rivoire, F. Hatami, J. Vučković, H. Park and M. D. Lukin, Preprint arXiv:1005.2204.

[26] T. B. Pittman, B. C. Jacobs and J. D. Franson, Opt. Comm. **246**, 545 (2004).

[27] Here we consider that dark counts in the detectors are, to a good approximation, independent of the incoming signals.

[28] Alternatively, one can also characterize Bob's detection setup using only one POVM which already includes the action of the polarization shifter.

[29] M. Curty and N. Lütkenhaus, Phys. Rev. A **69**, 042321 (2004).