Passive decoy-state quantum key distribution with practical light sources

Marcos Curty,[1] Xiongfeng Ma,[2] Bing Qi,[3] and Tobias Moroder[2,4,5]

[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*

[4]*Quantum Information Theory Group, Institute of Theoretical Physics I, University of Erlangen-Nürnberg, D-91058 Erlangen, Germany*

[5]*Max Planck Institute for the Science of Light, D-91058 Erlangen, Germany*

(Received 14 November 2009; published 10 February 2010)

Decoy states have been proven to be a very useful method for significantly enhancing the performance of quantum key distribution systems with practical light sources. Although active modulation of the intensity of the laser pulses is an effective way of preparing decoy states in principle, in practice passive preparation might be desirable in some scenarios. Typical passive schemes involve parametric down-conversion. More recently, it has been shown that phase-randomized weak coherent pulses (WCP) can also be used for the same purpose [M. Curty *et al.*, Opt. Lett. **34**, 3238 (2009).] This proposal requires only linear optics together with a simple threshold photon detector, which shows the practical feasibility of the method. Most importantly, the resulting secret key rate is comparable to the one delivered by an active decoy-state setup with an infinite number of decoy settings. In this article we extend these results, now showing specifically the analysis for other practical scenarios with different light sources and photodetectors. In particular, we consider sources emitting thermal states, phase-randomized WCP, and strong coherent light in combination with several types of photodetectors, like, for instance, threshold photon detectors, photon number resolving detectors, and classical photodetectors. Our analysis includes as well the effect that detection inefficiencies and noise in the form of dark counts shown by current threshold detectors might have on the final secret key rate. Moreover, we provide estimations on the effects that statistical fluctuations due to a finite data size can have in practical implementations.

DOI: 10.1103/PhysRevA.81.022310 PACS number(s): 03.67.Dd, 03.67.Hk, 03.67.Mn

I. INTRODUCTION

Quantum key distribution (QKD) is the first quantum information task that reaches the commercial market to offer efficient and user-friendly cryptographic systems providing an unprecedented level of security [1]. It 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 [2]. This secret key is the essential ingredient of the one-time-pad or Vernam cipher [3], the only known encryption method that can deliver information-theoretic secure communications.

Practical implementations of QKD are usually based on the transmission of phase randomized weak coherent pulses (WCP) with a typical average photon number of 0.1 or higher [4]. These states can be easily prepared using only standard semiconductor lasers and calibrated attenuators. The main drawback of these systems, however, arises from the fact that some signals may contain more than one photon prepared in the same quantum state. When this effect is combined with the considerable attenuation introduced by the quantum channel (about 0.2 dB/km), it opens an important security loophole. Eve can perform, for instance, the so-called *Photon Number Splitting* attack on the multiphoton pulses [5]. This attack provides her with full information about the part of the key generated with the multiphoton signals, without causing any disturbance in the signal polarization. As a result, it turns out that the standard BB84 protocol [6] with phase-randomized WCP can deliver a key generation rate of order $O(\eta^2)$, where η denotes the transmission efficiency of the quantum channel [7,8]. This poor performance contrasts with the one expected from a QKD scheme using a single-photon source, where the key generation rate scales linearly with η.

A significant improvement of the achievable secret key rate can be obtained if the original hardware is slightly modified. For instance, one can use the so-called decoy-state method [9–12], which can basically reach the performance of single-photon sources. The essential idea behind decoy-state QKD with phase-randomized WCP is quite simple: Alice varies, independently and randomly, the mean photon number of each signal state she sends to Bob by employing different intensity settings. This is typically realized by means of a variable optical attenuator (VOA) together with a random number generator. Eve does not know a priori the mean photon number of each signal state sent by Alice. This means that her eavesdropping strategy can only depend on the actual photon number of these signals, but not on the particular intensity setting used to generate them. From the measurement results corresponding to different intensity settings, the legitimate users can obtain a better estimation of the behavior of the quantum channel. This fact translates into an enhancement of the resulting secret key rate. The decoy-state technique has been successfully implemented in several recent experiments [13] that show the practical feasibility of this method.

Although active modulation of the intensity of the pulses suffices to perform decoy-state QKD in principle, in practice passive preparation might be desirable in some scenarios. For instance, in those experimental setups operating at high transmission rates. Passive schemes might also be more resistant to side channel attacks than active systems. For

example, if the VOA, which changes the intensity of Alice's pulses, is not properly designed, it may happen that some physical parameters of the pulses emitted by the sender depend on the particular setting selected. This fact could open a security loophole in the active schemes.

Known passive schemes rely typically on the use of a parametric down-conversion (PDC) source together with a photon detector [14–16]. The main idea behind these proposals comes from the photon number correlations that exist between the two output modes of a PDC source. By measuring the photon number distribution of one output mode it is possible to infer the photon number statistics of the other mode. In particular, Ref. [14] considers the case where Alice measures one of the output modes by means of a time-multiplexed detector (TMD), which provides photon number resolution capabilities [17]; Ref. [15] analyzes the scenario where the detector used by Alice is just a simple threshold detector, while the authors of Ref. [16] generalize the ideas introduced by Mauerer *et al.* in Ref. [14] to QKD setups using triggered PDC sources. All these schemes nearly reach the performance of a single-photon source.

More recently, it has been shown that phase-randomized WCP can also be used for the same purpose [18]; that is, one does not need a nonlinear optics network preparing entangled states. The crucial requirement of a passive decoy-state setup is to obtain correlations between the photon number statistics of different signals; hence it is sufficient that these correlations are classical. The main contribution of Ref. [18] is rather simple: When two phase-randomized coherent states interfere at a beam splitter (BS), the photon number statistics of the outcome signals are classically correlated. This effect contrasts with the one expected from the interference of two pure coherent states with fixed phase relation at a BS. In this last case, it is well known that the photon number statistics of the outcome signals is just the product of two Poissonian distributions. Now the idea is similar to that of Refs. [14–16]: By measuring one of the two outcome signals of the BS, the conditional photon number distribution of the other signal varies depending on the result obtained [18]. In the asymptotic limit of an infinite long experiment, it turns out that the secret key rate provided by such a passive scheme is similar to the one delivered by an active decoy-state setup with infinite decoy settings [18]. A similar result can also be obtained when Alice uses heralded single-photon sources showing non-Poissonian photon number statistics [19].

In this article we extend the results presented in Ref. [18], now showing specifically the analysis for other practical scenarios with different light sources and photodetectors. In particular, we consider sources emitting thermal states and phase-randomized WCP in combination with threshold detectors and photon number resolving (PNR) detectors. In the case of threshold detectors, we include as well the effect that detection inefficiencies and dark counts present in current measurement devices might have on the final secret key rate. For simplicity, these measurement imperfections were not considered in Ref. [18]. On the other hand, PNR detectors allow us to obtain ultimate lower bounds on the maximal performance that can be expected from these kinds of passive setups. We also present a passive scheme that employs strong coherent light and does not require the use of single-photon detectors, but can operate with a simpler classical photodetector. This fact makes this setup especially interesting from an experimental point of view. Finally, we provide an estimation on the effects that statistical fluctuations due to a finite data size can have in practical implementations.

The article is organized as follows. In Sec. II we review very briefly the concept of decoy-state QKD. Next, in Sec. III we present a simple model to characterize the behavior of a typical quantum channel. This model will be relevant later on, when we evaluate the performance of the different passive schemes that we present in the following sections. Our starting point is the basic passive decoy-state setup introduced in Ref. [18]. This scheme is explained very briefly in Sec. IV. Then, in Sec. V we analyze its security when Alice uses a source of thermal light. Sec. VI and Sec. VII consider the case where Alice employs a source of coherent light. First, Sec. VI investigates the scenario where the states prepared by Alice are phase-randomized WCP. Then, Sec. VII presents a passive decoy-state scheme that uses strong coherent light. In Sec. VIII we discuss the effects of statistical fluctuations. Finally, Sec. IX concludes the article with a summary.

II. DECOY-STATE QKD

In decoy-state QKD Alice prepares mixtures of Fock states with different photon number statistics and sends these states to Bob [9–12]. The photon number distribution of each signal state is chosen, independently and at random, from a set of possible predetermined settings. Let p_n^l denote the conditional probability that a signal state prepared by Alice contains n photons given that she selected setting l, with $l \in \{0, \ldots, m\}$. For instance, if Alice employs a source of phase-randomized WCP then $p_n^l = e^{-\mu_l}\mu_l^n/n!$, and she varies the mean photon number (intensity) μ_l of each signal. Assuming that Alice has chosen setting l, such states can be described as

$$\rho^l = \sum_{n=0}^{\infty} p_n^l |n\rangle\langle n|, \tag{1}$$

where $|n\rangle$ denote Fock states with n photons.

The gain Q^l corresponding to setting l, that is the probability that Bob obtains a click in his measurement apparatus when Alice sends him a signal state prepared with setting l, can be written as

$$Q^l = \sum_{n=0}^{\infty} p_n^l Y_n, \tag{2}$$

where Y_n denotes the yield of an n-photon signal (i.e., the conditional probability of a detection event on Bob's side given that Alice transmitted an n-photon state. Similarly, the quantum bit error rate (QBER) associated to setting l, which we shall denote as E^l, is given by

$$Q^l E^l = \sum_{n=0}^{\infty} p_n^l Y_n e_n, \tag{3}$$

with e_n representing the error rate of an n-photon signal.

Now the main idea of decoy-state QKD is very simple. From the observed data Q^l and E^l, together with the knowledge of the photon number distributions p_n^l, Alice and Bob can

estimate the value of the unknown parameters Y_n and e_n just by solving the set of linear equations given by Eqs. (2) and (3). For instance, in the general scenario where Alice employs an infinite number of possible decoy settings then she can estimate any finite number of parameters Y_n and e_n with arbitrary precision. On the other hand, if Alice and Bob are only interested in the value of a few probabilities (typically Y_0, Y_1, and e_1), then they can estimate them by means of only a few different decoy settings [10–12].

In this article we shall consider that Alice and Bob treat each decoy setting separately, and they distill the secret key from all of them. We use the security analysis presented in Ref. [10], which combines the results provided by Gottesman-Lo-Lütkenhaus-Preskill (GLLP) in Ref. [8] (see also Ref. [20]) with the decoy-state method. Specifically, the secret key rate formula can be written as

$$R \geqslant \sum_{l=0}^{m} \max\{R^l, 0\}, \tag{4}$$

where R^l satisfies

$$R^l \geqslant q\left\{-Q^l f(E^l) H(E^l) + p_1^l Y_1 [1 - H(e_1)] + p_0^l Y_0\right\}. \tag{5}$$

The parameter q is the efficiency of the protocol ($q = 1/2$ for the standard BB84 protocol [6], and $q \approx 1$ for its efficient version [21]); $f(E^l)$ is the efficiency of the error correction protocol as a function of the error rate E^l [22], typically $f(E^l) \geqslant 1$ with Shannon limit $f(E^l) = 1$; e_1 denotes the single-photon error rate; $H(x) = -x \log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function.

To apply the secret key rate formula given by Eq. (5) one needs to solve Eqs. (2) and (3) in order to estimate the quantities Y_0, Y_1, and e_1. For that, we shall use the procedure proposed in Ref. [12]. This method requires that the probabilities p_n^l satisfy certain conditions. It is important to emphasize, however, that the estimation technique presented in Ref. [12] only constitutes a possible example of a finite setting estimation procedure and no optimality statement is given. In principle, many other estimation methods are also available for this purpose, such as linear programming tools [23], which might result in sharper, or for the purpose of QKD, better bounds on the considered probabilities.

III. CHANNEL MODEL

In this section we present a simple model to describe the behavior of a typical quantum channel. This model will be relevant later on, when we evaluate the performance of the passive decoy-state setups that we present in the following sections. In particular, we shall consider the channel model used in Refs. [10,12]. This model reproduces a normal behavior of a quantum channel (i.e., in the absence of eavesdropping). Note, however, that the results presented in this article can also be applied to any other quantum channel, as they only depend on the observed gains Q^l and error rates E^l.

A. Yield

There are two main factors that contribute to the yield of an n-photon signal: the background rate Y_0, and the signal states sent by Alice. Usually Y_0 is, to a good approximation, independent of the signal detection. This parameter depends mainly on the dark count rate of Bob's detection apparatus, together with other background contributions, such as stray light coming from timing pulses that are not completely filtered out in reception. In the scenario considered, the yields Y_n can be expressed as [10,12]

$$Y_n = 1 - (1 - Y_0)(1 - \eta_{\text{sys}})^n, \tag{6}$$

where η_{sys} represents the overall transmittance of the system. This quantity can be written as

$$\eta_{\text{sys}} = \eta_{\text{channel}} \eta_{\text{Bob}}, \tag{7}$$

where η_{channel} is the transmittance of the quantum channel, and η_{Bob} denotes the overall transmittance of Bob's detection apparatus; that is, η_{Bob} includes the transmittance of any optical component within Bob's measurement device and the detector efficiency. The parameter η_{channel} can be related with a transmission distance d measured in km for the given QKD scheme as

$$\eta_{\text{channel}} = 10^{-\frac{\alpha d}{10}}, \tag{8}$$

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

B. Quantum bit error rate

The n-photon error rate e_n is given by [10,12]

$$e_n = \frac{Y_0 e_0 + (Y_n - Y_0) e_d}{Y_n}, \tag{9}$$

where e_d is the probability that a signal hits the wrong detector on Bob's side due to the misalignment in the quantum channel and in his detection setup. For simplicity, here we assume that e_d is a constant independent of the distance. Moreover, from now on we shall consider that the background is random (i.e., $e_0 = 1/2$).

IV. PASSIVE DECOY-STATE QKD SETUP

The basic setup is rather simple [18]. It is illustrated in Fig. 1. Suppose two Fock diagonal states

$$\begin{aligned} \rho &= \sum_{n=0}^{\infty} p_n |n\rangle\langle n|, \\ \sigma &= \sum_{n=0}^{\infty} r_n |n\rangle\langle n|, \end{aligned} \tag{10}$$

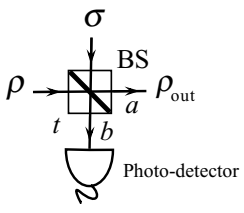

FIG. 1. Basic setup of a passive decoy-state QKD scheme: interference of two Fock diagonal states, ρ and σ, at a beam splitter (BS) of transmittance t; a and b represent the two output modes.

interfere at a BS of transmittance t. If the probabilities p_n and r_n are properly selected, then it turns out that the photon number distributions of the two outcome signals can be classically correlated. By measuring the signal state in mode b, therefore, the conditional photon number statistics of the signal state in mode a vary depending on the result obtained.

In the following sections we analyze the setup represented in Fig. 1 for different light sources and photodetectors. We start by considering a simple source of thermal states. Afterward, we investigate more practical sources of coherent light.

V. THERMAL LIGHT

Suppose that the signal state ρ, which appears in Fig. 1, is a thermal state of mean photon number μ. Such a state can be written as

$$\rho = \frac{1}{1+\mu}\sum_{n=0}^{\infty}\left(\frac{\mu}{1+\mu}\right)^n |n\rangle\langle n|, \tag{11}$$

and let σ be a vacuum state. In this scenario, the joint probability of having n photons in output mode a and m photons in output mode b (see Fig. 1) has the form

$$p_{n,m} = \frac{1}{1+\mu}\binom{n+m}{m}\left(\frac{\mu}{1+\mu}\right)^{n+m} t^n(1-t)^m, \tag{12}$$

that is, depending on the result of Alice's measurement in mode b, the conditional photon number distribution of the signals in mode a varies.

In particular, we have that whenever Alice ignores the result of her measurement, the total probability of finding n photons in mode a can be expressed as

$$p_n^t = \sum_{m=0}^{\infty} p_{n,m} = \frac{1}{1+\mu t}\left(\frac{\mu t}{1+\mu t}\right)^n. \tag{13}$$

Next, we consider the case where Alice uses a threshold detector to measure mode b.

A. Threshold detector

Such a detector can be characterized by a positive operator value measure (POVM) that contains two elements, F_{vac} and F_{click}, given by [24]

$$\begin{aligned} F_{\text{vac}} &= (1-\epsilon)\sum_{n=0}^{\infty}(1-\eta_{\text{d}})^n|n\rangle\langle n|, \\ F_{\text{click}} &= \mathbb{1} - F_{\text{vac}}. \end{aligned} \tag{14}$$

The parameter η_{d} denotes the detection efficiency of the detector, and ϵ represents its probability of having a dark count. Equation (14) assumes that ϵ is, to a good approximation, independent of the incoming signals. The outcome of F_{vac} corresponds to "no click" in the detector, whereas the operator F_{click} gives precisely one detection "click", which means at least one photon is detected.

The joint probability for seeing n photons in mode a and no click in the threshold detector, which we shall denote as $p_n^{\bar{c}}$, has the form

$$p_n^{\bar{c}} = (1-\epsilon)\sum_{m=0}^{\infty}(1-\eta_{\text{d}})^m p_{n,m} = \frac{(1-\epsilon)}{r}\left(\frac{\mu t}{r}\right)^n, \tag{15}$$

with the parameter r given by

$$r = 1 + \mu[t + (1-t)\eta_{\text{d}}]. \tag{16}$$

If the detector produces a click, the joint probability of finding n photons in mode a is given by

$$p_n^c = p_n^t - p_n^{\bar{c}}. \tag{17}$$

Figure 2 shows the conditional photon number statistics of the outcome signal in mode a depending on the result of the threshold detector (click and not click): $q_n^c = p_n^c/(1-N_{\text{th}})$ and $q_n^{\bar{c}} = p_n^{\bar{c}}/N_{\text{th}}$, with

$$N_{\text{th}} = \sum_{n=0}^{\infty} p_n^{\bar{c}} = \frac{1-\epsilon}{1+\mu\eta_{\text{d}}(1-t)}. \tag{18}$$

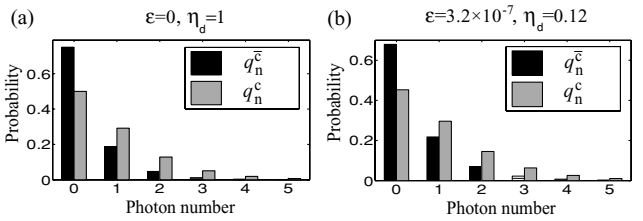

FIG. 2. Conditional photon number distribution in mode a (see Fig. 1): $q_n^{\bar{c}}$ (black) versus q_n^c (gray) when ρ is given by Eq. (11), and σ is a vacuum state. We use $\mu = 1$ and $t = 1/2$, and we study two situations: (a) a perfect threshold photon detector (i.e., $\epsilon = 0$ and $\eta_{\text{d}} = 1$), and (b) $\epsilon = 3.2 \times 10^{-7}$ and $\eta_{\text{d}} = 0.12$. These last data correspond to the experiment reported by Gobby *et al.* in Ref. [25].

B. Lower bound on the secret key rate

We consider that Alice and Bob distill secret key both from click and no-click events. The calculations to estimate the yields Y_0 and Y_1, together with the single-photon error rate e_1, are included in Appendix A.

For simulation purposes we use the channel model described in Sec. III. After substituting Eqs. (6)–(9) into the gain and QBER formulas we obtain that the parameters $Q^{\bar{c}}$, $E^{\bar{c}}$, Q^t, and E^t can be written as

$$\begin{aligned} Q^{\bar{c}} &= N_{\text{th}} - \frac{(1-\epsilon)(1-Y_0)}{r-(1-\eta_{\text{sys}})\mu t}, \\ Q^{\bar{c}}E^{\bar{c}} &= (e_0 - e_d)Y_0 N_{\text{th}} + e_d Q^{\bar{c}}, \\ Q^t &= \frac{Y_0 + \mu t\eta_{\text{sys}}}{1+\mu t\eta_{\text{sys}}}, \\ Q^t E^t &= (e_0 - e_d)Y_0 + e_d Q^t, \end{aligned} \tag{19}$$

where $Q^c = Q^t - Q^{\bar{c}}$ and $Q^c E^c = Q^t E^t - Q^{\bar{c}} E^{\bar{c}}$.

The resulting lower bound on the secret key rate is illustrated in Fig. 3 (dashed line). We employ the experimental parameters reported by Gobby *et al.* in Ref. [25]: $Y_0 = 1.7 \times 10^{-6}$, $e_d = 0.033$, $\alpha = 0.21$ dB/km, and Bob's detection efficiency $\eta_{\text{Bob}} = 0.045$. We further assume that

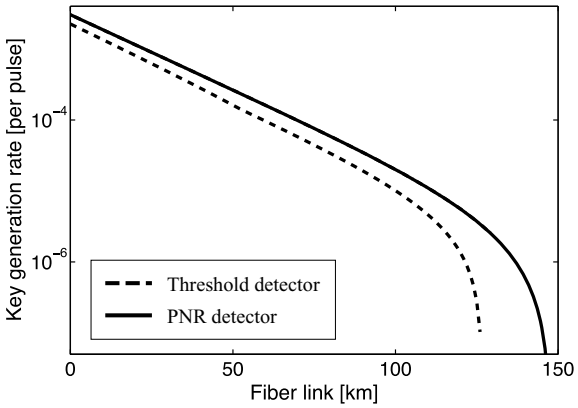

FIG. 3. Lower bound on the secret key rate R given by Eq. (4) in logarithmic scale for the passive decoy-state setup illustrated in Fig. 1 with two intensity settings. The signal state ρ is given by Eq. (11), and σ is a vacuum state. We consider two possible scenarios: (Case A) a perfect threshold detector (i.e., $\epsilon = 0$ and $\eta_{\rm d} = 1$), and (Case B) $\epsilon = 3.2 \times 10^{-7}$ and $\eta_{\rm d} = 0.12$ [25]. Both cases provide approximately the same final key rate and they cannot be distinguished with the resolution of this figure (dashed line). The solid line represents a lower bound on R when Alice employs a PNR detector instead of a threshold detector (see Appendix B1).

$q = 1$, and $f(E^c) = f(E^{\bar{c}}) = 1.22$. These data are used as well for simulation purposes in the following sections. We study two different scenarios: (Case A) a perfect threshold detector, (i.e., $\epsilon = 0$ and $\eta_{\rm d} = 1$), and (Case B) $\epsilon = 3.2 \times 10^{-7}$ and $\eta_{\rm d} = 0.12$ [25]. In both cases we find that the values of the mean photon number μ and the transmittance t, which maximize the secret key rate formula, are quite similar and almost constant with the distance. In particular, μ is quite strong (around 200 in the simulation), while t is quite weak (around 10^{-3}). This result is not surprising. When $\mu \gg 1$ and $t \ll 1$, Alice's threshold detector produces a click most of the time. Then, in the few occasions where Alice actually does not see a click in her measurement device, she can be quite confident that the signal state that goes to Bob is quite weak. Note that in this scenario the conditional photon number statistics $q_n^{\bar{c}}$ satisfy $q_0^{\bar{c}} \approx 1$ and $q_{n\geqslant 1}^{\bar{c}} \approx 0$. Similarly to the one weak decoy-state protocol proposed in Ref. [12], this fact allows Alice and Bob to obtain an accurate estimation of Y_1 and e_1, which results in an enhancement of the achievable secret key rate and distance. The cutoff point where the secret key rate drops down to zero is $l \approx 126$ km.

One can improve the resulting secret key rate further by using a passive scheme with more intensity settings. For instance, Alice may employ a PNR detector instead of a threshold detector, or she could use several threshold detectors in combination with beam splitters. (In this context, see also Ref. [16]). Figure 3 also illustrates this last scenario, for the case where Alice uses a PNR detector (solid line). As expected, it turns out that now the legitimate users can estimate the actual value of the relevant parameters Y_0, Y_1, and e_1 with arbitrary precision (see Appendix B1). The cutoff point where the secret key rate drops down to zero is $l \approx 147$ km. This result shows that the performance of the passive setup represented in Fig. 1 with a threshold detector is already close to the best performance that can be achieved with such a scheme and the security analysis provided in Refs. [8,20].

VI. WEAK COHERENT LIGHT

Suppose now that the signal states ρ and σ that appear in Fig. 1 are two phase-randomized WCP emitted by a pulsed laser source, that is

$$\begin{aligned} \rho &= e^{-\mu_1} \sum_{n=0}^{\infty} \frac{\mu_1^n}{n!} |n\rangle\langle n|, \\ \sigma &= e^{-\mu_2} \sum_{n=0}^{\infty} \frac{\mu_2^n}{n!} |n\rangle\langle n|, \end{aligned} \tag{20}$$

with μ_1 and μ_2 denoting, respectively, the mean photon number of the two signals. In this scenario, the joint probability of having n photons in output mode a and m photons in output mode b can be written as [18]

$$p_{n,m} = \frac{\upsilon^{n+m} e^{-\upsilon}}{n!m!} \frac{1}{2\pi} \int_0^{2\pi} \gamma^n (1-\gamma)^m d\theta, \tag{21}$$

where the parameters υ, γ, and ξ, are given by

$$\begin{aligned} \upsilon &= \mu_1 + \mu_2, \\ \gamma &= \frac{\mu_1 t + \mu_2 (1-t) + \xi \cos\theta}{\upsilon}, \\ \xi &= 2\sqrt{\mu_1 \mu_2 (1-t) t}. \end{aligned} \tag{22}$$

This result differs from the one expected from the interference of two pure coherent states with fixed phase relation, $|\sqrt{\mu_1} e^{i\phi_1}\rangle$ and $|\sqrt{\mu_2} e^{i\phi_2}\rangle$, at a BS of transmittance t. In this last case, $p_{n,m}$ is just the product of two Poissonian distributions. Whenever Alice ignores the result of her measurement in mode b, then the probability of finding n photons in mode a can be expressed as

$$p_n^t = \sum_{m=0}^{\infty} p_{n,m} = \frac{\upsilon^n}{n!} \frac{1}{2\pi} \int_0^{2\pi} \gamma^n e^{-\upsilon\gamma} d\theta, \tag{23}$$

which turns out to be a non-Poissonian probability distribution [18]. Let us now consider the case where Alice uses a threshold detector to measure output mode b.

A. Threshold detector

The analysis is completely analogous to the one presented in Sec. V A. In particular, the joint probability for seeing n photons in mode a and no click in the threshold detector now has the form

$$\begin{aligned} p_n^{\bar{c}} &= (1-\epsilon) \sum_{m=0}^{\infty} (1-\eta_{\rm d})^m p_{n,m} \\ &= (1-\epsilon) \frac{\upsilon^n e^{-\eta_{\rm d}\upsilon}}{n!} \frac{1}{2\pi} \int_0^{2\pi} \gamma^n e^{-(1-\eta_{\rm d})\upsilon\gamma} d\theta. \end{aligned} \tag{24}$$

On the other hand, if the detector produces a click, the joint probability of finding n photons in mode a is given by Eq. (17). Figures 4(a) and 4(b) show the conditional photon number statistics of the outcome signal in mode a depending on the

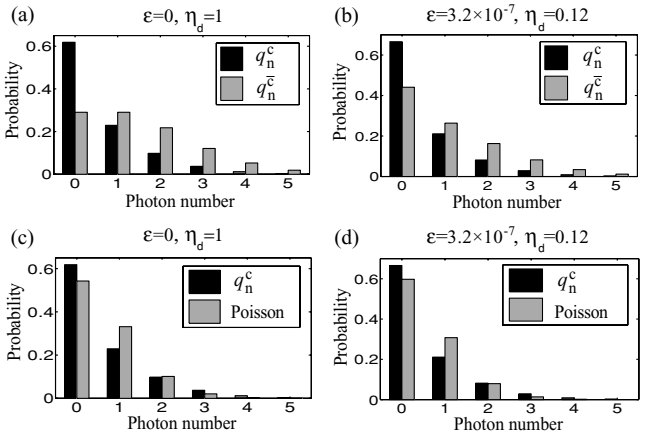

FIG. 4. Conditional photon number distribution in mode a (see Fig. 1): q_n^c (black) versus $q_n^{\bar{c}}$ (gray) when the signal states ρ and σ are two phase-randomized WCP given by Eq. (20). We consider that $\mu_1 = \mu_2 = 1$ and $t = 1/2$, and we study two situations: (a) a perfect threshold photon detector (i.e., $\epsilon = 0$ and $\eta_{\rm d} = 1$ [18]), and (b) $\epsilon = 3.2 \times 10^{-7}$ and $\eta_{\rm d} = 0.12$. These last data correspond to the experiment reported by Gobby *et al.* in Ref. [25]. (c) and (d) represent q_n^c (black) versus a Poissonian distribution of the same mean photon number for the two scenarios described above (perfect and imperfect threshold photon detector).

result of the detector (click and no click): $q_n^c = p_n^c/(1 - N_{\rm w})$ and $q_n^{\bar{c}} = p_n^{\bar{c}}/N_{\rm w}$, with

$$N_{\rm w} = \sum_{n=0}^{\infty} p_n^{\bar{c}} = (1-\epsilon) e^{-\eta_{\rm d}[\mu_1(1-t)+\mu_2 t]} I_{0,\eta_{\rm d}\xi}, \tag{25}$$

and where $I_{q,z}$ represents the modified Bessel function of the first kind [26]. This function is defined as [26]

$$I_{q,z} = \frac{1}{2\pi i} \oint e^{(z/2)(t+1/t)} t^{-q-1} dt. \tag{26}$$

Figures 4(c) and 4(d) include as well a comparison between q_n^c and a Poissonian distribution of the same mean photon number. Both distributions, q_n^c and $q_n^{\bar{c}}$, are also non-Poissonian.

B. Lower bound on the secret key rate

To apply the secret key rate formula given by Eq. (5), with $l \in \{c, \bar{c}\}$, we need to estimate the quantities Y_0, Y_1, and e_1. For that, we follow the same procedure explained in Appendix A. This method requires that p_n^t and $p_n^{\bar{c}}$ satisfy certain conditions that we confirmed numerically. As a result, it turns out that the bounds given by Eqs. (A10)–(A16) are also valid in this scenario.

The only relevant statistics to evaluate Eqs. (A10)–(A16) are p_n^t and $p_n^{\bar{c}}$, with $n = 0, 1, 2$. These probabilities can be obtained by solving Eqs. (23) and (24). They are given in Appendix C. Note that p_n^c can be directly calculated from these two statistics by means of Eq. (17). After substituting Eqs. (6)–(9) into the gain and QBER formulas we obtain

$$Q^{\bar{c}} = N_{\rm w} - (1-\epsilon)(1-Y_0) e^{(\eta_{\rm d}-\eta_{\rm sys})\omega - \eta_{\rm d}\upsilon} \times I_{0,(\eta_{\rm d}-\eta_{\rm sys})\xi},$$
$$Q^{\bar{c}} E^{\bar{c}} = (e_0 - e_d) Y_0 N_{\rm w} + e_d Q^{\bar{c}},$$
$$Q^t = 1 - (1-Y_0) e^{-\eta_{\rm sys}\omega} I_{0,\eta_{\rm sys}\xi},$$
$$Q^t E^t = (e_0 - e_d) Y_0 + e_d Q^t, \tag{27}$$

with the parameter ω given by

$$\omega = \mu_1 t + \mu_2 (1-t). \tag{28}$$

The resulting lower bound on the secret key rate is illustrated in Fig. 5. We assume that $t = 1/2$ (i.e., we consider a simple 50 : 50 BS). Again, we study two different situations: (Case A) $\epsilon = 0$ and $\eta_{\rm d} = 1$ [18], and (Case B) $\epsilon = 3.2 \times 10^{-7}$ and $\eta_{\rm d} = 0.12$ [25]. In both cases the optimal values of the intensities μ_1 and μ_2 are almost constant with the distance. One of them is quite weak (around 10^{-4}), while the other one is around 0.5. The reason for this result can be understood as follows. When the intensity of one of the signals is really weak, the output photon number distributions in mode a are always close to a Poissonian distribution (for click and no-click events). This distribution is narrower than the one arising when both μ_1 and μ_2 are of the same order of magnitude. In this case, a better estimation of Y_1 and e_1 can be derived, and this fact translates into a higher secret key rate. It must be emphasized, however, that from an experimental point of view this solution might not be optimal, especially because in this scenario the two output distributions p_n^c and $p_n^{\bar{c}}$ might be too close to each other for being distinguished in practice. This effect could be especially relevant when one considers statistical fluctuations due to finite data size (see Sec. VIII); for instance, small fluctuations in a practical system could overwhelm the tiny difference between the decoy state and the signal state in this case. Figure 5 includes as well the secret key rate of an active asymptotic decoy-state QKD system with infinite

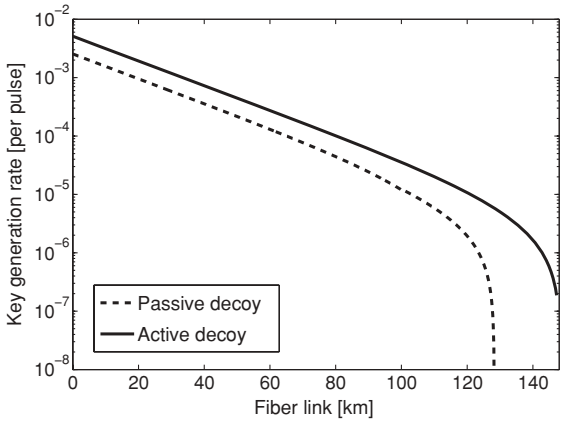

FIG. 5. Lower bound on the secret key rate R given by Eq. (4) in logarithmic scale for the passive decoy-state setup illustrated in Fig. 1 with two intensity settings. The signal states ρ and σ are two phase-randomized WCP given by Eq. (20). The transmittance of the BS is $t = 1/2$. We consider two possible scenarios: (Case A) $\epsilon = 0$ and $\eta_{\rm d} = 1$ [18] (i.e., a perfect threshold photon detector), and (Case B) $\epsilon = 3.2 \times 10^{-7}$ and $\eta_{\rm d} = 0.12$ [25]. Both cases provide approximately the same final key rate and they cannot be distinguished with the resolution of this figure (dashed line). The solid line represents a lower bound on R for an active asymptotic decoy-state system with infinite decoy settings [10]. This last result coincides approximately with the case where Alice employs a PNR detector (see Appendix B2), and the secret key rate in both scenarios cannot be distinguished with the resolution of this figure.

decoy settings [10]. The cutoff points where the secret key rate drops down to zero are $l \approx 128$ km (passive setup with two intensity settings) and $l \approx 147$ km (active asymptotic setup). From these results we see that the performance of the passive scheme with a threshold detector is comparable to the active one, thus showing the practical interest of the passive setup.

As in Sec. V, one can improve the performance of the passive scheme further by using more intensity settings. The case where Alice uses a PNR detector is analyzed in Appendix B2. The result is also shown in Fig. 5. It reproduces approximately the behavior of the asymptotic active setup and the secret key rate in both scenarios cannot be distinguished with the resolution of this figure (solid line). This result is not surprising, since in both situations (passive and active) we apply Eq. (5) with the actual values of the parameters Y_0, Y_1, and e_1. The only difference between these two setups arises from the photon number distribution of the signal states that go to Bob. In particular, while in the passive scheme the relevant statistics are given by Eq. (B9), in the active setup these statistics have the form given by Eq. (B12).

C. Alternative implementation scheme

The passive setup illustrated in Fig. 1 requires that Alice employ two independent sources of signal states. This fact might become especially relevant when she uses phase-randomized WCP since, in this situation, none of the signal states entering the BS can be the vacuum state. Otherwise, the photon number distributions of the output signals in mode a and mode b would be statistically independent.

Alternatively to the passive scheme shown in Fig. 1, Alice could as well employ, for instance, the scheme illustrated in Fig. 6. This setup has only one laser diode, but follows a similar spirit as the original scheme in Fig. 1, where a photodetector is used to measure the output signals in mode b. It includes, however, an intensity modulator (IM) to block either all the even or all the odd pulses in mode a. This requires, therefore, an active control of the functioning of the IM, but note that no random number generator is needed here. The main reason for blocking half of the pulses in mode a is to suppress possible correlations between them; that is, the action of the IM guarantees that the signal states that go to Bob are tensor products of mixtures of Fock states. Then, one can directly apply the security analysis provided in Refs. [8,10,20]. Thanks to the one-pulse delay introduced by one arm of the interferometer, together with a proper selection of the transmittance t_1, it can be shown that both setups in

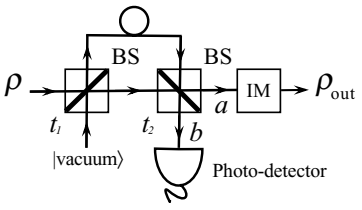

FIG. 6. Alternative implementation scheme with only one pulsed laser source. The delay introduced by one arm of the interferometer is equal to the time difference between two pulses. The intensity modulator (IM) blocks either all the even or all the odd optical pulses in mode a.

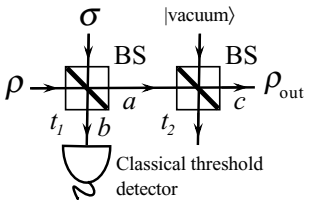

FIG. 7. Basic setup of a passive decoy-state QKD scheme with strong coherent light. The mean photon number of the signal states ρ and σ is now quite high; for instance, $\approx 10^8$ photons. t_1 and t_2 represent the transmittances of the two BS's, and a, b, and c denote output modes.

Figs. 1 and 6 are completely equivalent, except from the resulting secret key rate. More precisely, the secret key rate in the active scheme is half the one of the passive setup, since half of the pulses are now discarded.

VII. STRONG COHERENT LIGHT

Let us now consider the passive decoy-state setup illustrated in Fig. 7. This scheme presents two main differences with respect to the passive system analyzed in Sec. VI. In particular, the mean photon number (intensity) of the signal states ρ and σ is now very high; for instance, $\approx 10^8$ photons. This fact allows Alice to use a simple classical photodetector to measure the pulses in mode b, which makes this scheme specially suited for experimental implementations. Moreover, it has an additional BS of transmittance t_2 to attenuate the signal states in mode a and bring them to the QKD regimen.

Due to the high intensity of the input signal states ρ and σ, we can describe the action of the first BS in Fig. 7 by means of a classical model. Specifically, let I_1 (I_2) represent the intensity of the input states ρ (σ), and let $I_a(\theta)$ [$I_b(\theta)$] be the intensity of the output pulses in mode a (b). Here the angle θ is just a function of the relative phase between the two input states. It is given by

$$\theta = \phi_1 - \phi_2 + \pi/2, \tag{29}$$

where ϕ_1 (ϕ_2) denotes the phase of the signal ρ (σ). As in Sec. VI, we assume that these phases are uniformly distributed between 0 and 2π for each pair of input states. This can be achieved, for instance, if Alice uses two pulsed laser sources to prepare the signals ρ and σ. With this notation, we have that $I_a(\theta)$ and $I_b(\theta)$ can be expressed as

$$\begin{aligned} I_a(\theta) &= t_1 I_1 + r_1 I_2 + 2\sqrt{t_1 r_1 I_1 I_2}\cos\theta, \\ I_b(\theta) &= r_1 I_1 + t_1 I_2 - 2\sqrt{t_1 r_1 I_1 I_2}\cos\theta, \end{aligned} \tag{30}$$

where t_1 denotes the transmittance of the BS, and $r_1 = 1 - t_1$.

A. Classical threshold detector

For simplicity, we shall consider that Alice uses a *perfect* classical threshold detector to measure the pulses in mode b. For each incoming signal, this device tells her whether its intensity is below or above a certain threshold value I_M that satisfies $I_b(\pi) > I_M > I_b(0)$; that is, the value of I_M is between the minimal and maximal possible values of the intensity of the pulses in mode b. Note, however, that the analysis presented in

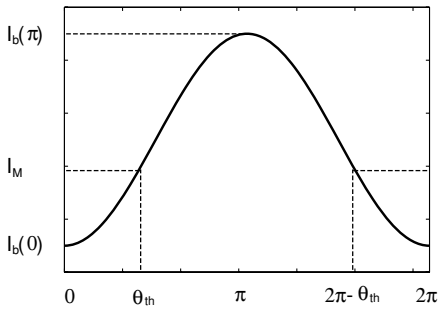

FIG. 8. Graphical representation of the intensity $I_b(\theta)$ in mode b (see Fig. 7) versus the angle θ. I_M represents the threshold value of the classical threshold detector, and θ_{th} is its associated threshold angle.

this section can be straightforwardly adapted to cover also the case of an imperfect classical threshold detector, or a classical photodetector with several threshold settings. Figure 8 shows a graphical representation of $I_b(\theta)$ versus the angle θ, together with the threshold value I_M. The angle θ_{th}, which satisfies $I_b(\theta_{\text{th}}) = I_M$, is given by

$$\theta_{\text{th}} = \arccos\left(\frac{r_1 I_1 + t_1 I_2 - I_M}{2\sqrt{t_1 r_1 I_1 I_2}}\right). \tag{31}$$

Whenever the classical threshold detector provides Alice with an intensity value below I_M, it turns out that the unnormalized signal states in mode c can be expressed as

$$\begin{aligned}\rho_{\text{out}}^{<I_M} &= \frac{1}{2\pi}\sum_{n=0}^{\infty}\left\{\int_0^{\theta_{\text{th}}}\frac{e^{-I_a(\theta)t_2}[I_a(\theta)t_2]^n}{n!}|n\rangle\langle n|d\theta\right.\\ &\quad\left.+\int_{2\pi-\theta_{\text{th}}}^{2\pi}\frac{e^{-I_a(\theta)t_2}[I_a(\theta)t_2]^n}{n!}|n\rangle\langle n|d\theta\right\}\\ &= \frac{1}{\pi}\sum_{n=0}^{\infty}\int_0^{\theta_{\text{th}}}\frac{e^{-I_a(\theta)t_2}[I_a(\theta)t_2]^n}{n!}|n\rangle\langle n|d\theta.\end{aligned} \tag{32}$$

This means, in particular, that the joint probability of finding n photons in mode c and an intensity value below I_M in mode b is given by

$$p_n^{<I_M} = \frac{t_2^n}{n!\pi}\int_0^{\theta_{\text{th}}} I_a(\theta)^n e^{-I_a(\theta)t_2}d\theta. \tag{33}$$

Similarly, we find that $p_n^{>I_M}$ can be written as

$$p_n^{>I_M} = \frac{t_2^n}{n!\pi}\int_{\theta_{\text{th}}}^{\pi} I_a(\theta)^n e^{-I_a(\theta)t_2}d\theta. \tag{34}$$

Figure 9(a) shows the conditional photon number statistics of the outcome signal in mode c depending on the result of the classical threshold detector (below or above I_M): $q_n^{<I_M} = p_n^{<I_M}/N_{\text{s}}$ and $q_n^{>I_M} = p_n^{>I_M}/(1-N_{\text{s}})$, with

$$N_{\text{s}} = \sum_{n=0}^{\infty} p_n^{<I_M} = \frac{\theta_{\text{th}}}{\pi}. \tag{35}$$

This figure includes as well a comparison between $q_n^{<I_M}$ (b) and $q_n^{>I_M}$ (c) and a Poissonian distribution of the same mean photon number. It turns out that both distributions, $q_n^{<I_M}$ and $q_n^{>I_M}$, approach a Poissonian distribution when t_2 is sufficiently small.

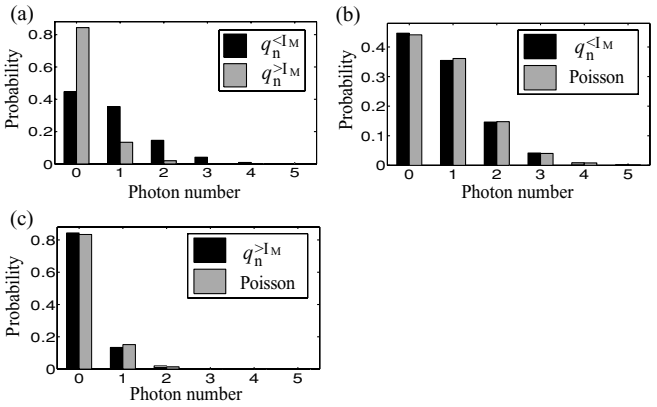

FIG. 9. (a) Conditional photon number distribution in mode c (see Fig. 7): $q_n^{<I_M}$ (black) and $q_n^{>I_M}$ (gray) for the case $I_1 = I_2 = I_M = 10^8$, $t_1 = 1/2$, and $t_2 = 0.5 \times 10^{-8}$. (b) and (c) represent, respectively, $q_n^{<I_M}$ and $q_n^{>I_M}$ (black) versus a Poissonian distribution of the same mean photon number (gray).

B. Lower bound on the secret key rate

Again, to apply the secret key rate formula given by Eq. (5), with $l \in \{< I_M, > I_M\}$, we need to estimate the quantities Y_0, Y_1, and e_1. Once more, we follow the procedure explained in Appendix A. We confirmed numerically that the probabilities $p_n^{<I_M}$ and $p_n^{>I_M}$ satisfy the conditions required to use this technique. As a result, it turns out that the bounds given by Eqs. (A10)–(A16) are also valid in this scenario.

For simplicity, we impose $I_1 = I_2 = I_M \equiv I$. This means that $\theta_{\text{th}} = \pi/2$. The relevant statistics $p_n^{<I_M}$ and $p_n^{>I_M}$, with $n = 0, 1, 2$, are calculated in Appendix D. After substituting Eqs. (6)–(9) into the gain and QBER formulas we obtain

$$\begin{aligned}Q^{<I_M} &= N_{\text{s}} - \frac{(1-Y_0)e^{-\eta_{\text{sys}}\kappa}}{2}(I_{0,\eta_{\text{sys}}\zeta} - L_{0,\eta_{\text{sys}}\zeta}),\\ Q^{<I_M}E^{<I_M} &= (e_0 - e_d)Y_0 N_{\text{s}} + e_d Q^{<I_M},\\ Q^{>I_M} &= (1-N_{\text{s}}) - \frac{(1-Y_0)e^{-\eta_{\text{sys}}\kappa}}{2}\\ &\quad\times(I_{0,\eta_{\text{sys}}\zeta} + L_{0,\eta_{\text{sys}}\zeta}),\\ Q^{>I_M}E^{>I_M} &= (e_0 - e_d)Y_0(1-N_{\text{s}}) + e_d Q^{>I_M},\end{aligned} \tag{36}$$

where the parameter κ is given by

$$\kappa = I t_2, \tag{37}$$

and $L_{q,z}$ represents the modified Struve function [27] defined by Eq. (D2).

The resulting lower bound on the secret key rate is illustrated in Fig. 10. We study two different situations: (Case A) We impose $t_1 = 1/2$ (i.e., we consider a simple 50 : 50 BS and we optimize the parameter κ), and (Case B) we optimize both quantities, t_1 and κ. In both scenarios the optimal values of the parameters are almost constant with the distance. In

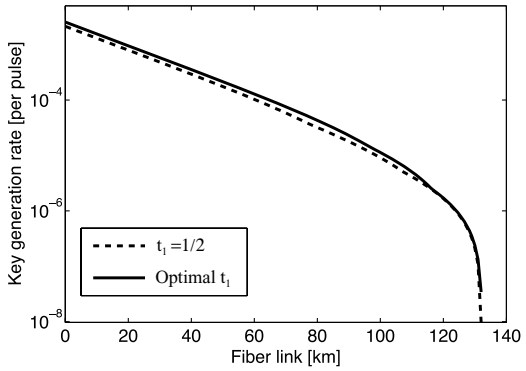

FIG. 10. Lower bound on the secret key rate R given by Eq. (4) in logarithmic scale for the passive decoy-state setup illustrated in Fig. 7 with two intensity settings. We consider two possible scenarios: (Case A) We impose $t_1 = 1/2$ [i.e., we consider a simple 50 : 50 BS and we optimize the parameter κ (dashed line)], and (Case B) we optimize both parameters, t_1 and κ (solid line).

the first case κ is around 0.2, whereas in the second case we obtain that t_1 and κ are, respectively, around 0.06 and 0.25. The solid line curve (Case B) shows a small discontinuity in its slope around 114 km. This discontinuity arises from the two secret key rate terms that are contained in Eq. (4) (i.e., for click and no-click events). The cutoff point where the secret key rate drops down to zero is $l \approx 132$ km in both Cases A and B. These results seem to indicate that this passive scheme can offer a better performance than the passive setups analyzed in Sec. V and Sec. VI with a threshold photon detector. This fact arises mainly from the probability distributions $p_n^{<I_M}$ and $p_n^{>I_M}$, which, in this scenario, approach a Poissonian distribution when t_2 is sufficiently small. Again, one can improve the performance of this system even further just by using more threshold settings in the classical threshold detector. Moreover, from an experimental point of view, this configuration might be more feasible than using PNR detectors.

To conclude this section, let us mention that (as in Sec. VI C) Alice could as well employ, for instance, the alternative active scheme illustrated in Fig. 11. This setup has only one pulsed laser source, but includes an intensity modulator (IM) to block either all the even or all the odd pulses in mode c. The argumentation here goes exactly the same as in Sec. VI C and we omit it for simplicity. The resulting secret key rate in the active scheme is half the one of the passive setup.

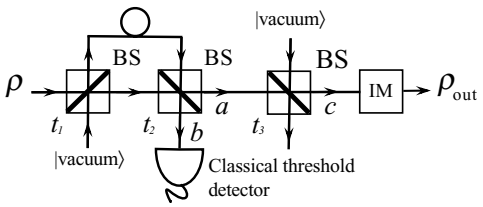

FIG. 11. Alternative implementation scheme with only one pulsed laser source. The delay introduced by one arm of the interferometer is equal to the time difference between two pulses. The intensity modulator (IM) blocks either the even or the odd optical pulses in mode c.

VIII. STATISTICAL FLUCTUATIONS

In this section, we discuss briefly the effect that finite data size in real life experiments might have on the final secret key rate. For that, we follow the statistical fluctuation analysis presented in Ref. [12]. This procedure is based on standard error analysis; that is, we shall assume that all the variables that are measured in the experiment fluctuate around their asymptotic values.

Our main objective here is to obtain a lower bound on the secret key rate formula given by Eq. (5) under statistical fluctuations. For that, we realize the following four assumptions:

1. Alice and Bob know the photon number statistics of the source well and we do not consider their fluctuations directly. Intuitively speaking, these fluctuations are included in the parameters measuring the gains and QBERs.
2. Alice and Bob use a real upper bound on the single-photon error rate e_1, thus no fluctuations have to be considered for this parameter. In particular, we use the fact that the number of errors within the single-photon states cannot be greater than the total number of errors.
3. Alice and Bob use a standard error analysis procedure to deal with the fluctuations of the variables that are measured.
4. The error rate of background does not fluctuate (i.e., $e_0 = 1/2$).

To illustrate our results, we focus on the passive decoy-state setup introduced in Sec. VI. Note, however, that a similar analysis can also be applied to the other passive schemes presented in this article.

A. Active decoy-state QKD

In order to make a fair comparison between the active and the passive decoy-state QKD setups with two intensity settings, from now on we shall consider an active scheme with only one decoy state [12]. In this last case, the quantities Y_1 and e_1 can be bounded as

$$Y_1 \geqslant Y_1^L = \frac{\mu^2 Q_\nu e^\nu - \nu^2 Q_\mu e^\mu - (\mu^2 - \nu^2) Y_0}{\mu\nu(\mu - \nu)},$$
$$e_1 \leqslant e_1^U = \frac{E_\mu Q_\mu e^\mu - e_0 Y_0}{Y_1^l \mu}, \tag{38}$$

where μ (ν) denotes the mean photon number of a signal (decoy) state, Q_μ (Q_ν) and E_μ (E_ν) represent, respectively, its associated gain and QBER, and Y_0 is a free parameter. Using the channel model described in Sec. III, we find that these parameters can be written as

$$Q_\mu = Y_0 + 1 - e^{-\mu\eta_{\rm sys}},$$
$$E_\mu Q_\mu = e_0 Y_0 + e_d(1 - e^{-\mu\eta_{\rm sys}}),$$
$$Q_\nu = Y_0 + 1 - e^{-\nu\eta_{\rm sys}}, \tag{39}$$
$$E_\nu Q_\nu = e_0 Y_0 + e_d(1 - e^{-\nu\eta_{\rm sys}}).$$

If we now apply a standard error analysis to these quantities we obtain that their deviations from the theoretical values are

given by

$$\begin{aligned}\Delta_{Q\mu} &= u_\alpha\sqrt{Q_\mu/N_\mu},\\ \Delta_{Q\nu} &= u_\alpha\sqrt{Q_\nu/N_\nu},\\ \Delta_{Q\mu E\mu} &= u_\alpha\sqrt{2E_\mu Q_\mu/N_\mu},\\ \Delta_{Q\nu E\nu} &= u_\alpha\sqrt{2E_\nu Q_\nu/N_\nu},\end{aligned} \tag{40}$$

where N_μ (N_ν) denotes the number of signal (weak decoy) pulses sent by Alice, and u_α represents the number of standard deviations from the central values; that is, the total number of pulses emitted by the source is just given by $N = N_\mu + N_\nu$. Roughly speaking, this means, for instance, that the gain of the signal states lies in the interval $Q_\mu \pm \Delta_{Q\mu}$ except with small probability, and similarly for the other quantities defined in Eq. (39). For example, if we select $u_\alpha = 10$, then the corresponding confidence interval is $1 - 1.5 \times 10^{-23}$, which we use later on for simulation purposes. For simplicity, here we have assumed that Alice and Bob use the standard BB84 protocol (i.e., they keep only half of their raw bits due to the basis sift). This is the reason for the factor 2 that appears in the last two expressions of Eq. (40). In this context, see also Ref. [28] for a discussion on the optimal value of the parameter q.

B. The background Y_0

The bounds given by Eq. (38) depend on the unknown parameter Y_0. When a vacuum decoy state is applied, the value of Y_0 can be estimated. Alternatively, one can also derive a lower bound on Y_1 and an upper bound on e_1 that do not depend on Y_0. Specifically, from Eqs. (2) and (3) we obtain

$$\begin{aligned}(1-2e_1)Y_1 \geqslant A = &\frac{\mu}{\nu(\mu-\nu)}Q_\nu(1-2E_\nu)e^\nu\\ &-\frac{\nu}{\mu(\mu-\nu)}Q_\mu(1-2E_\mu)e^\mu.\end{aligned} \tag{41}$$

The gains Q_μ and Q_ν, together with the QBERs E_μ and E_ν, are directly measured in the experiment, and their statistical fluctuations are given by Eq. (40). On the other hand, we have

$$e_1 \leqslant \frac{B}{Y_1^L}, \tag{42}$$

with the parameter B given by

$$B = \min\left\{\frac{E_\nu Q_\nu e^\nu}{\nu}, \frac{E_\mu Q_\mu e^\mu - E_\nu Q_\nu e^\nu}{\mu-\nu}\right\}. \tag{43}$$

Combining Eqs. (41) and (42) we find

$$Y_1[1-H(e_1)] \geqslant \frac{A}{1-2e_1}\left[1 - H\left(\frac{B(1-2e_1)}{A}\right)\right]. \tag{44}$$

The quantities A and B can be obtained directly from the variables measured in the experiment. Moreover, if one considers the secret key rate formula given by Eq. (5) as a function of the free parameter e_1, then one should select an upper bound on e_1, which gives a value (may not be a bound) for Y_1 as

$$\begin{aligned}Y_1^t &= A + 2B,\\ e_1^U &= \frac{B}{A+2B},\end{aligned} \tag{45}$$

where the equation for e_1^U comes from solving the two inequalities given by Eqs. (41) and (42).

Again, using a standard error analysis procedure, we find that the deviations of the parameters A and B from their theoretical values can be written as

$$\begin{aligned}\Delta_A &= [(c_1\Delta_{Q\nu})^2 + 4(c_1\Delta_{E\nu Q\nu})^2 + (c_2\Delta_{Q\mu})^2\\ &\quad + 4(c_2\Delta_{E\mu Q\mu})^2]^{\frac{1}{2}},\\ \Delta_B &= \min\left\{\frac{e^\mu\Delta_{E\mu Q\mu}}{\mu}, \frac{e^\nu\Delta_{E\nu Q\nu}}{\nu},\right.\\ &\quad \left.\frac{\sqrt{(e^\mu\Delta_{E\mu Q\mu})^2 + (e^\nu\Delta_{E\nu Q\nu})^2}}{\mu-\nu}\right\},\end{aligned} \tag{46}$$

where the coefficients c_1 and c_2 have the form

$$\begin{aligned}c_1 &= \frac{\mu}{\nu(\mu-\nu)}e^\nu,\\ c_2 &= \frac{\nu}{\mu(\mu-\nu)}e^\mu,\end{aligned} \tag{47}$$

and the deviations of the gains and the QBERs are given by Eq. (40).

For simplicity, we assume now that A and B are statistically independent. Thus, the statistical deviation of the crucial term $Y_1[1-H_2(e_1)]$ in the secret key formula can be written as

$$\begin{aligned}\Delta_{Y_1[1-H_2(e_1)]} = &\left\{\left[\Delta_A \log_2\left(\frac{2A+2B}{A+2B}\right)\right]^2\right.\\ &\left.+\left[\Delta_B \log_2\left(\frac{4B(A+B)}{(A+2B)^2}\right)\right]^2\right\}^{\frac{1}{2}}.\end{aligned} \tag{48}$$

From Eqs. (40), (46), and (48) one can directly calculate the final secret key rate with statistical fluctuations for an active decoy-state setup with only one decoy state [12]. The result is illustrated in Fig. 12 (dashed line). Here we use again the experimental data reported by Gobby *et al.* in Ref. [25]. Moreover, we pick the data size (total number of pulses emitted by Alice) to be $N = 6 \times 10^9$. We calculate the optimal values of μ and ν for each fiber length numerically. It turns out that both parameters are almost constant with the distance. One of them is weak (it varies between 0.03 and 0.06), while the other is around 0.48. This figure includes as well the resulting secret key rate for the same setup without considering statistical fluctuations (thick solid line). The cutoff points where the secret key rate drops down to zero are $l \approx 129.5$ km (active setup with statistical fluctuations) and $l \approx 147$ km (active setup without considering statistical fluctuations). From these results we see that the performance of this active scheme is quite robust against statistical fluctuations.

C. Passive decoy-state QKD

The analysis is completely analogous to the previous section. Specifically, we find that the parameters A and B

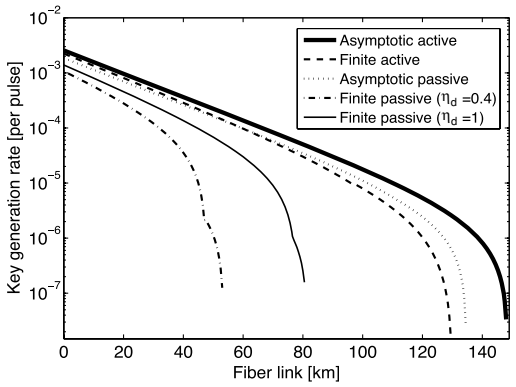

FIG. 12. Lower bound on the secret key rate R given by Eq. (4) in logarithmic scale. We consider four possible scenarios: an active decoy-state setup (with only one decoy state) with statistical fluctuations (dashed line) [12]; an active decoy-state setup (with only one decoy state) without considering statistical fluctuations (thick solid line) [12]; the passive decoy-state scheme with WCP introduced in Sec. VI now considering statistical fluctuations [in this last case, moreover, we study two possible situations depending on the value of $\eta_{\rm d}$: $\eta_{\rm d}=1$ (thin solid line), and $\eta_{\rm d}=0.4$ (dash-dotted line)]; the passive decoy-state scheme with WCP introduced in Sec. VI with $\eta_{\rm d}=1$ and without considering statistical fluctuations (dotted line). In all passive setups the transmittance of the BS is $t=1/2$ and we use $\epsilon=0$. Furthermore, we pick the data size (total number of pulses emitted by Alice) to be $N=6\times10^9$. The confidence interval for statistical fluctuations is 10 standard deviations (i.e., $1-1.5\times10^{-23}$).

are now given by

$$A=\frac{p_2^{\bar c}Q^t(1-2E^t)-p_2^tQ^{\bar c}(1-2E^{\bar c})}{p_2^{\bar c}p_1^t-p_2^tp_1^{\bar c}},$$
$$B=\min\left\{\frac{E^{\bar c}Q^{\bar c}}{p_1^{\bar c}},\frac{p_0^{\bar c}E^tQ^t-p_0^tE^{\bar c}Q^{\bar c}}{p_0^{\bar c}p_1^t-p_0^tp_1^{\bar c}}\right\}, \tag{49}$$

while Eq. (45) is still valid in this scenario. The deviations of A and B have the form

$$\Delta_A=\frac{1}{p_2^{\bar c}p_1^t-p_2^tp_1^{\bar c}}\Big[\big(p_2^{\bar c}\Delta_{Q^t}\big)^2+4\big(p_2^{\bar c}\Delta_{E^tQ^t}\big)^2 +\big(p_2^t\Delta_{Q^{\bar c}}\big)^2+4\big(p_2^t\Delta_{E^{\bar c}Q^{\bar c}}\big)\Big]^{\frac12}, \tag{50}$$
$$\Delta_B=\min\left\{\frac{\Delta_{E^tQ^t}}{p_1^t},\frac{\Delta_{E^{\bar c}Q^{\bar c}}}{p_1^{\bar c}},\frac{\sqrt{\big(p_0^{\bar c}\Delta_{E^tQ^t}\big)^2+\big(p_0^t\Delta_{E^{\bar c}Q^{\bar c}}\big)^2}}{p_0^{\bar c}p_1^t-p_0^tp_1^{\bar c}}\right\}.$$

On the other hand, the deviations of the gains and the QBERs can now be written as

$$\Delta_{Q^t}=u_\alpha\sqrt{Q^t/N},$$
$$\Delta_{Q^{\bar c}}=u_\alpha\sqrt{Q^{\bar c}/N^{\bar c}},$$
$$\Delta_{E^tQ^t}=u_\alpha\sqrt{2E^tQ^t/N}, \tag{51}$$
$$\Delta_{E^{\bar c}Q^{\bar c}}=u_\alpha\sqrt{2E^{\bar c}Q^{\bar c}/N^{\bar c}},$$

where $N^{\bar c}$ denotes the number of pulses where Alice obtained no click in her threshold detector, and N is the total number of pulses emitted by the source. The deviation of the term $Y_1[1-H_2(e_1)]$ is again given by Eq. (48).

The secret key rate for the passive decoy-state scheme with WCP introduced in Sec. VI with two intensity settings and considering statistical fluctuations is illustrated in Fig. 12. We assume that $t=1/2$ (i.e., we consider a simple 50 : 50 BS) and $\epsilon=0$. The data size is equal to that of the previous section (i.e., $N=6\times10^9$). We study two different situations depending on the efficiency of Alice's threshold detector: $\eta_{\rm d}=1$ (thin solid line) and $\eta_{\rm d}=0.4$ (dash-dotted line). In both cases the optimal values of the intensities μ_1 and μ_2 are almost constant with the distance. One of them is weak (it varies between 0.1 and 0.17), while the other is around 0.5. The reason for the discontinuity that appears in the slope of these two lines is the same as in Fig. 10 [i.e., it comes from the two secret key rate terms that are included in Eq. (4)]. Figure 12 contains as well the resulting secret key rate for the same setup with $\eta_{\rm d}=1$ and without considering statistical fluctuations (dotted line). The cutoff points where the secret key rate drops down to zero are $l\approx53$ km (passive setup with statistical fluctuations and $\eta_{\rm d}=0.4$), $l\approx80$ km (passive setup with statistical fluctuations and $\eta_{\rm d}=1$), and $l\approx128$ km (passive setup without considering statistical fluctuations; see Sec. VI). From these results we see that the performance of the passive schemes introduced in Sec. VI (with statistical fluctuations) depends on the actual value of the efficiency $\eta_{\rm d}$. In particular, when Alice's detector efficiency is low, the photon number statistics of the signal states that go to Bob (conditioned on Alice's detection) become close to each other. This effect becomes especially relevant when one considers statistical fluctuations due to finite data size. In this last case, small fluctuations can easily cover the difference between the signal states associated, respectively, to click and no-click events on Alice's threshold detector. As a result, the achievable secret key rate and distance decrease.

IX. CONCLUSION

In this article we have extended the results presented in Ref. [18], now showing specifically the analysis for other practical scenarios with different light sources and photodetectors. In particular, we have considered sources emitting thermal states and phase-randomized WCP in combination with threshold detectors and photon number resolving detectors. In the case of threshold detectors, we have included as well the effect that detection inefficiencies and dark counts present in current measurement devices might have on the final secret key rate. For simplicity, these measurement imperfections were not considered in the original proposal. On the other hand, PNR detectors have allowed us to obtain ultimate lower bounds on the maximal performance that can be expected from these kinds of passive setups. We have also presented a passive scheme that employs strong coherent light and does not require the use of single-photon detectors, but can operate with a simpler classical photodetector. This fact makes this setup specially interesting from an experimental point of view. Finally, we have provided an estimation on the effects that statistical fluctuations due to a finite data size can have in practical implementations.

ACKNOWLEDGMENTS

The authors thank H.-K. Lo, N. Lütkenhaus, and Y. Zhao for very useful discussions and, in particular, M. Koashi for pointing out a reference. M. C. especially thanks the University of Toronto and the Institute for Quantum Computing (University of Waterloo) for hospitality and support during his stay in both institutions. This work was supported by the European Projects SECOQC and QAP, by the Natural Sciences and Engineering Research Council of Canada Discovery Grant, Quantum Works, CSEC, and by Xunta de Galicia, Spain (Grant No. INCITE08PXIB322257PR).

APPENDIX A: ESTIMATION PROCEDURE

Our starting point is the secret key rate formula given by Eq. (5). This expression can be lower bounded by

$$R^l \geqslant q\{-Q^l f(E^l)H(E^l)+(p_1^l Y_1 + p_0^l Y_0)[1 - H(e_1^U)]\}, \tag{A1}$$

where e_1^U denotes an upper bound on the single-photon error rate e_1. Hence, for our purposes it is enough to obtain a lower bound on the quantities $p_1^l Y_1 + p_0^l Y_0$ for all l, together with e_1^U. For that, we follow the estimation procedure proposed in Ref. [12]. Next, we show the explicit calculations for the case where Alice uses the passive scheme introduced in Sec. V.

A. Lower bound on $p_1^l Y_1 + p_0^l Y_0$

The method contains two main steps. First, we have $p_1^l Y_1 + p_0^l Y_0$ always satisfies

$$p_1^l Y_1 + p_0^l Y_0 \geqslant p_1^l Y_1^L + p_0^l Y_0, \tag{A2}$$

for all $l \in \{c, \bar{c}\}$, and where Y_1^L denotes a lower bound on the yield of a single-photon state. To find Y_1^L, note that

$$\begin{aligned} p_2^t Q^{\bar{c}} - p_2^{\bar{c}} Q^t &= \sum_{n=0}^{\infty} (p_2^t p_n^{\bar{c}} - p_2^{\bar{c}} p_n^t) Y_n \\ &\leqslant \sum_{n=0}^{1} (p_2^t p_n^{\bar{c}} - p_2^{\bar{c}} p_n^t) Y_n, \end{aligned} \tag{A3}$$

since

$$p_2^t p_n^{\bar{c}} - p_2^{\bar{c}} p_n^t = \frac{(1-\epsilon)(\mu t)^{n+2}}{[(1+\mu t)r]^3}\left(\frac{1}{r^{n-2}} - \frac{1}{(1+\mu t)^{n-2}}\right) \leqslant 0, \tag{A4}$$

for all $n \geqslant 2$, and where the parameter r is given by Eq. (16). To see this, note that the first term on the right-hand side of Eq. (A4) is always greater than or equal to zero, and $r \geqslant 1 + \mu t \geqslant 1$. Similarly, we have $p_2^t p_n^{\bar{c}} - p_2^{\bar{c}} p_n^t \geqslant 0$ for all $n \leqslant 1$. Combining both results, we obtain

$$Y_1 \geqslant Y_1^L = \max\left\{\frac{p_2^t Q^{\bar{c}} - p_2^{\bar{c}} Q^t - (p_2^t p_0^{\bar{c}} - p_2^{\bar{c}} p_0^t) Y_0}{p_2^t p_1^{\bar{c}} - p_2^{\bar{c}} p_1^t}, 0\right\}. \tag{A5}$$

Now comes the second step. The term that multiplies Y_0 in the expression $p_1^l Y_1^L + p_0^l Y_0$ satisfies

$$-p_1^l \frac{p_2^t p_0^{\bar{c}} - p_2^{\bar{c}} p_0^t}{p_2^t p_1^{\bar{c}} - p_2^{\bar{c}} p_1^t} + p_0^l \leqslant 0. \tag{A6}$$

This last statement can be proven as follows. The condition given by Eq. (A6) is equivalent to

$$p_0^l (p_2^t p_1^{\bar{c}} - p_2^{\bar{c}} p_1^t) \leqslant p_1^l (p_2^t p_0^{\bar{c}} - p_2^{\bar{c}} p_0^t), \tag{A7}$$

since, as we have seen above, $p_2^t p_1^{\bar{c}} - p_2^{\bar{c}} p_1^t \geqslant 0$. After a short calculation, it turns out that Eq. (A7) can be further simplified to

$$p_1^t p_0^{\bar{c}} - p_1^{\bar{c}} p_0^t \geqslant 0, \tag{A8}$$

both for $l = c$ and $l = \bar{c}$. Finally, from the definition of the probabilities p_n^t and $p_n^{\bar{c}}$ given by Eqs. (13)–(15), we find

$$p_1^t p_n^{\bar{c}} - p_1^{\bar{c}} p_n^t = \frac{(1-\epsilon)(\mu t)^{n+1}}{[(1+\mu t)r]^2}\left(\frac{1}{r^{n-1}} - \frac{1}{(1+\mu t)^{n-1}}\right), \tag{A9}$$

which is greater than or equal to zero for all $n \leqslant 1$, and negative otherwise. Note that the first term on the right-hand side of Eq. (A9) is always greater than or equal to zero, and the sign of the second term depends on the value of n, since $r \geqslant 1 + \mu t \geqslant 1$.

We obtain, therefore,

$$\begin{aligned} p_1^l Y_1 + p_0^l Y_0 \geqslant \max\Bigg\{ &\frac{p_1^l (p_2^t Q^{\bar{c}} - p_2^{\bar{c}} Q^t)}{p_2^t p_1^{\bar{c}} - p_2^{\bar{c}} p_1^t} \\ &+ \left[p_0^l - p_1^l \frac{p_2^t p_0^{\bar{c}} - p_2^{\bar{c}} p_0^t}{p_2^t p_1^{\bar{c}} - p_2^{\bar{c}} p_1^t}\right] Y_0^u, 0\Bigg\}, \end{aligned} \tag{A10}$$

for all $l \in \{c, \bar{c}\}$, and where Y_0^u denotes an upper bound on the background rate Y_0. This parameter can be calculated from Eq. (3). In particular, we have

$$Q^c E^c = \sum_{n=0}^{\infty} p_n^c Y_n e_n \geqslant p_0^c Y_0 e_0, \tag{A11}$$

and similarly for the product $Q^{\bar{c}} E^{\bar{c}}$. We find

$$Y_0 \leqslant Y_0^u = \min\left\{\frac{E^c Q^c}{p_0^c e_0}, \frac{E^{\bar{c}} Q^{\bar{c}}}{p_0^{\bar{c}} e_0}\right\}. \tag{A12}$$

B. Upper bound on e_1

For this, we proceed as follows:

$$\begin{aligned} p_0^{\bar{c}} Q^t E^t - p_0^t Q^{\bar{c}} E^{\bar{c}} &= \sum_{n=1}^{\infty} (p_n^t p_0^{\bar{c}} - p_n^{\bar{c}} p_0^t) Y_n e_n \\ &\geqslant (p_1^t p_0^{\bar{c}} - p_1^{\bar{c}} p_0^t) Y_1 e_1, \end{aligned} \tag{A13}$$

where the inequality condition comes from the fact that

$$p_n^t p_0^{\bar{c}} - p_n^{\bar{c}} p_0^t = \frac{(1-\epsilon)(\mu t)^n}{(1+\mu t)r}\left(\frac{1}{(1+\mu t)^n} - \frac{1}{r^n}\right) \geqslant 0, \tag{A14}$$

for all $n \geqslant 1$. From Eq. (A13) we obtain, therefore, that e_1 is upper bounded by $(p_0^{\bar{c}} E^t Q^t - p_0^t E^{\bar{c}} Q^{\bar{c}})/[(p_1^t p_0^{\bar{c}} - p_1^{\bar{c}} p_0^t) Y_1^L]$, where Y_1^L is given by Eq. (A5) with the parameter Y_0 replaced by Y_0^u.

On the other hand, note that Eq. (3) also provides a simple upper bound on e_1. Specifically,

$$Q^c E^c = \sum_{n=0}^{\infty} p_n^c Y_n e_n \geqslant p_0^c Y_0 e_0 + p_1^c Y_1 e_1, \tag{A15}$$

and similarly for the product $Q^{\bar{c}} E^{\bar{c}}$. Putting all these conditions together, we find that

$$e_1 \leqslant e_1^U = \min \left\{ \frac{E^c Q^c - p_0^c Y_0^L e_0}{p_1^c Y_1^L}, \frac{E^{\bar{c}} Q^{\bar{c}} - p_0^{\bar{c}} Y_0^L e_0}{p_1^{\bar{c}} Y_1^L}, \frac{p_0^{\bar{c}} E^t Q^t - p_0^t E^{\bar{c}} Q^{\bar{c}}}{(p_1^t p_0^{\bar{c}} - p_1^{\bar{c}} p_0^t) Y_1^L} \right\}, \tag{A16}$$

where Y_0^L represents a lower bound on the background rate Y_0. To calculate this parameter we use the following inequality:

$$\begin{aligned} p_1^t Q^{\bar{c}} - p_1^{\bar{c}} Q^t &= (p_1^t p_0^{\bar{c}} - p_1^{\bar{c}} p_0^t) Y_0 + \sum_{n=2}^{\infty} (p_1^t p_n^{\bar{c}} - p_1^{\bar{c}} p_n^t) Y_n \\ &\leqslant (p_1^t p_0^{\bar{c}} - p_1^{\bar{c}} p_0^t) Y_0, \end{aligned} \tag{A17}$$

since, as we have seen above, $p_1^t p_n^{\bar{c}} - p_1^{\bar{c}} p_n^t \leqslant 0$ for all $n \geqslant 2$. From Eq. (A17) we obtain, therefore,

$$Y_0 \geqslant Y_0^L = \max \left\{ \frac{p_1^t Q^{\bar{c}} - p_1^{\bar{c}} Q^t}{p_1^t p_0^{\bar{c}} - p_1^{\bar{c}} p_0^t}, 0 \right\}. \tag{A18}$$

APPENDIX B: PNR DETECTOR

In this Appendix we study the case where Alice uses a *perfect* PNR detector to measure the signal states in mode b. The main goal of this analysis is to obtain an ultimate lower bound on the secret key rate that can be achieved with the passive decoy-state setups introduced in Sec. V and Sec. VI, in combination with the security analysis provided in Refs. [8,20].

A perfect PNR detector can be characterized by a POVM that contains an infinite number of elements,

$$F_m = |m\rangle\langle m|, \tag{B1}$$

with $m = 0, 1, \ldots, \infty$. The outcome of F_m corresponds to the detection of m photons in mode b.

1. Thermal light

Let us begin by considering the passive scheme analyzed in Sec. V with Alice using a PNR detector. Whenever she finds m photons in mode b, then the joint probability distribution of having n photons in mode a is just given by Eq. (12). Figure 13 shows the conditional photon number statistics in mode a given that mode b contains exactly m photons: $p_n^m = p_{n,m}/N_m$, with

$$N_m = \sum_{n=0}^{\infty} p_{n,m} = \frac{1}{1+\mu(1-t)} \left[\frac{\mu(1-t)}{1+\mu(1-t)} \right]^m. \tag{B2}$$

In this scenario, it turns out that Alice and Bob can always estimate any finite number of yields Y_n and error rates e_n with

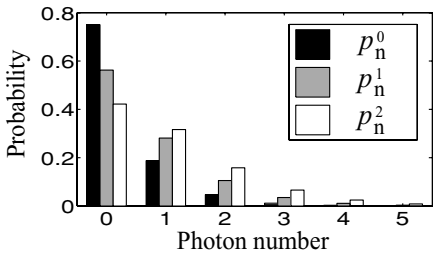

FIG. 13. Conditional photon number distribution in mode a when Alice uses a PNR detector, ρ is given by Eq. (11), and σ is a vacuum state: p_n^0 (black), p_n^1 (gray), and p_n^2 (white). We consider that $\mu = 1$, $t = 1/2$, and $n \leqslant 5$.

arbitrary precision. In particular, they can obtain the actual values of the parameters Y_0, Y_1, and e_1. To see this, let Q^m denote the overall gain of the signal states sent to Bob when mode b contains exactly m photons, and let the parameters X_m and V_n be defined as

$$\begin{aligned} X_m &= \frac{(1+\mu)^{m+1} Q^m}{[\mu(1-t)]^m}, \\ V_n &= \left(\frac{\mu t}{1+\mu} \right)^n Y_n. \end{aligned} \tag{B3}$$

With this notation, and using the definition of $p_{n,m}$ given by Eq. (12), we find that Eq. (2) can be rewritten as

$$X_m = \sum_{n=0}^{\infty} \binom{n+m}{m} V_n, \tag{B4}$$

that is, the coefficient matrix of the system of linear equations given by Eq. (B4) for all possible values of m is a symmetric Pascal matrix [29]. This matrix has determinant equal to one and, therefore, in principle can always be inverted [29]. Then, from the knowledge of the coefficients V_n, the legitimate users can directly obtain the values of the yields Y_n by means of Eq. (B3). A similar argument can also be used to show that Alice and Bob can obtain as well the values of e_n.

After substituting Eqs. (6)–(9) into the gain and QBER formulas we obtain

$$\begin{aligned} Q^m &= N_m - \frac{(1-Y_0)[\mu(1-t)]^m}{\{1+\mu[1-(1-\eta_{\mathrm{sys}})t]\}^{m+1}}, \\ Q^m E^m &= (e_0 - e_d) Y_0 N_m + e_d Q^m. \end{aligned} \tag{B5}$$

In order to evaluate Eq. (5) we need to find the probabilities $p_{0,m}$ and $p_{1,m}$ for all m. From Eq. (12) we have that these parameters can be expressed as

$$\begin{aligned} p_{0,m} &= \frac{[\mu(1-t)]^m}{(1+\mu)^{m+1}}, \\ p_{1,m} &= \frac{(m+1)t(1-t)^m}{1+\mu} \left(\frac{\mu}{1+\mu} \right)^{m+1}. \end{aligned} \tag{B6}$$

The resulting lower bound on the secret key rate is illustrated in Fig. 3 (solid line). The optimal values of the parameters μ and t are quite constant with the distance. Specifically, in this figure we choose μ around 18.5 and t around 0.02.

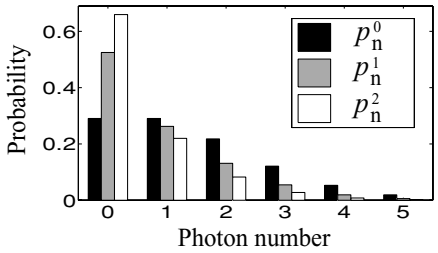

FIG. 14. Conditional photon number distribution in mode a when Alice uses a PNR detector: p_n^0 (black), p_n^1 (gray), and p_n^2 (white). The signal states ρ and σ in Fig. 1 are two phase-randomized WCP given by Eq. (20). We consider that $\mu_1 = \mu_2 = 1$, $t = 1/2$, and $n \leqslant 5$.

2. Weak coherent light

Let us now consider the passive scheme illustrated in Sec. VI with Alice using a PNR detector. Whenever her detector finds m photons in mode b, the joint probability distribution of having n photons in mode a is given by Eq. (21). Figure 14 shows the conditional photon number statistics in mode a given that mode b contains exactly m photons: $p_n^m = p_{n,m}/N_m$, with

$$N_m = \sum_{n=0}^{\infty} p_{n,m} = \frac{\upsilon^m e^{-\upsilon}}{m!}\frac{1}{2\pi}\int_0^{2\pi}(1-\gamma)^m e^{\upsilon\gamma}d\theta. \tag{B7}$$

To show that the experimental observations associated with different outcomes of the PNR detector allow Alice and Bob to obtain the values of the parameters Y_0, Y_1, and e_1 with arbitrary precision, one could follow the same procedure explained in Appendix B1; that is, one could try to prove that the determinant of the coefficient matrices associated with the systems of linear equations given by Eqs. (2) and (3) is different from zero also in this scenario. For simplicity, here we have confirmed this statement only numerically.

After substituting Eqs. (6)–(9) into the gain and QBER formulas we obtain

$$\begin{aligned} Q^m &= \frac{\upsilon^m e^{-\upsilon}}{m!}\frac{1}{2\pi}\int_0^{2\pi}[1-(1-Y_0)e^{-\eta_{\rm sys}\upsilon\gamma}](1-\gamma)^m e^{\upsilon\gamma}d\theta, \\ Q^m E^m &= (e_0 - e_d)Y_0 N_m + e_d Q^m. \end{aligned} \tag{B8}$$

The relevant probabilities $p_{0,m}$ and $p_{1,m}$ can be calculated directly from Eq. (21). We find that

$$\begin{aligned} p_{0,m} &= \frac{e^{-\upsilon}(\upsilon-\omega)^m}{\Gamma_{1+m}} g\left[\frac{1-m}{2}, -\frac{m}{2}, 1, \frac{\xi^2}{(\upsilon-\omega)^2}\right], \\ p_{1,m} &= \omega p_{0,m} - \frac{e^{-\upsilon}\xi^2(\upsilon-\omega)^{m-1}}{2\Gamma_m} \\ &\quad \times g\left[\frac{1-m}{2}, 1-\frac{m}{2}, 2, \frac{\xi^2}{(\upsilon-\omega)^2}\right], \end{aligned} \tag{B9}$$

where the Gamma function Γ_z is defined as [26]

$$\Gamma_z = \int_0^{\infty} t^{z-1}e^{-t}dt, \tag{B10}$$

and where $g(a,b,c,z)$ represents the hypergeometric function [26]. This function is defined as [26]

$$g(a,b,c,z) = \frac{\Gamma_c}{\Gamma_b\Gamma_{c-b}}\int_0^1 \frac{t^{b-1}(1-t)^{c-b-1}}{(1-tz)^a}dt. \tag{B11}$$

In this case, the lower bound on the resulting secret key rate reproduces approximately the behavior of the asymptotic active decoy-state setup illustrated in Fig. 5 (solid line). Here we have assumed again that $t = 1/2$. The values of the intensities μ_1 and μ_2, which optimize the secret key rate formula, are, respectively, $\approx 10^{-4}$ and ≈ 0.95. As already discussed in Sec. VI, this result is not surprising since the only difference between both setups (passive and active) arises from the photon number probabilities of the signal states sent by Alice. Although in the passive scheme the relevant statistics are given by Eq. (B9), in the active setup they have the form

$$\begin{aligned} p_{0,m} &= e^{-\mu_m}, \\ p_{1,m} &= e^{-\mu_m}\mu_m, \end{aligned} \tag{B12}$$

with μ_m denoting the mean photon number of the signals associated with setting m. Still, it turns out that this difference is not significant enough to be appreciated with the resolution of Fig. 5 when we optimize the parameters μ_1 and μ_2.

APPENDIX C: WEAK COHERENT LIGHT: PROBABILITIES p_n^t AND $p_n^{\bar{c}}$

In this Appendix we provide explicit expressions for the probabilities p_n^t and $p_n^{\bar{c}}$, with $n = 0, 1, 2$, for the case of a passive decoy-state setup with phase-randomized WCP. After a short calculation, we find that

$$\begin{aligned} p_0^t &= I_{0,\xi}e^{-\omega}, \\ p_1^t &= (\omega I_{0,\xi} - \xi I_{1,\xi})e^{-\omega}, \\ p_2^t &= \tfrac{1}{2}[\omega^2 I_{0,\xi} + (1-2\omega)\xi I_{1,\xi} + \xi^2 I_{2,\xi}]e^{-\omega}, \end{aligned} \tag{C1}$$

with $\omega = \mu_1 t + \mu_2(1-t)$. The probabilities $p_n^{\bar{c}}$ have the form

$$\begin{aligned} p_0^{\bar{c}} &= \tau I_{0,(1-\eta_{\rm d})\xi}, \\ p_1^{\bar{c}} &= \tau[\omega I_{0,(1-\eta_{\rm d})\xi} - \xi I_{1,(1-\eta_{\rm d})\xi}], \\ p_2^{\bar{c}} &= \frac{\tau}{2}\left[\omega^2 I_{0,(1-\eta_{\rm d})\xi} + \left(\frac{1}{1-\eta_{\rm d}} - 2\omega\right)\xi I_{1,(1-\eta_{\rm d})\xi} \right. \\ &\quad \left. + \xi^2 I_{2,(1-\eta_{\rm d})\xi}\right], \end{aligned} \tag{C2}$$

where $\tau = (1-\epsilon)e^{-[\eta_{\rm d}\upsilon + (1-\eta_{\rm d})\omega]}$.

APPENDIX D: PROBABILITIES $p_n^{<I_M}$ AND $p_n^{>I_M}$

In this Appendix we provide explicit expressions for the probabilities $p_n^{<I_M}$ and $p_n^{>I_M}$, with $n = 0, 1, 2$. For simplicity, we impose $I_1 = I_2 = I_M \equiv I$. After a short calculation, we obtain

$$\begin{aligned} p_0^{<I_M} &= \frac{e^{-\kappa}}{2}(I_{0,\zeta} - L_{0,\zeta}), \\ p_1^{<I_M} &= \frac{e^{-\kappa}}{2}[\kappa(I_{0,\zeta} - L_{0,\zeta}) - \zeta(I_{1,\zeta} - L_{-1,\zeta})], \end{aligned} \tag{D1}$$

$$p_2^{<I_M} = \frac{e^{-\kappa}}{4}\left\{\kappa^2(I_{0,\zeta} - L_{0,\zeta}) + \zeta\left[\frac{2}{\pi}\left(1 - \frac{\zeta^2}{3}\right) + (1-2\kappa)(I_{1,\zeta} - L_{-1,\zeta}) + \zeta(I_{2,\zeta} - L_{2,\zeta})\right]\right\},$$

where $\kappa = It_2$, $\zeta = 2\kappa\sqrt{t_1 r_1}$, and $L_{q,z}$ represents the modified Struve function [27]. This function is defined as [27]

$$L_{q,z} = \frac{z^q}{2^{q-1}\sqrt{\pi}\Gamma_{q+1/2}}\int_0^{\pi/2}\sinh(z\cos\theta)\sin\theta^{2q}d\theta. \quad \text{(D2)}$$

On the other hand, the probabilities $p_n^{>I_M}$ have the form

$$\begin{aligned} p_0^{>I_M} &= \frac{e^{-\kappa}}{2}(I_{0,\zeta} + L_{0,\zeta}), \\ p_1^{>I_M} &= \frac{e^{-\kappa}}{2}[\kappa(I_{0,\zeta} + L_{0,\zeta}) - \zeta(I_{1,\zeta} + L_{-1,\zeta})], \\ p_2^{>I_M} &= \frac{e^{-\kappa}}{4}\left\{\kappa^2(I_{0,\zeta} + L_{0,\zeta}) + \zeta\left[-\frac{2}{\pi}\left(1 - \frac{\zeta^2}{3}\right) + (1-2\kappa)(I_{1,\zeta} + L_{-1,\zeta}) + \zeta(I_{2,\zeta} + L_{2,\zeta})\right]\right\}. \end{aligned} \quad \text{(D3)}$$

[1] idQuantique, Geneva, Switzerland, www.idquantique.com; MagiQ Technologies, New York, www.magiqtech.com; Smartquantum, Lannion, France, www.smartquantum.com.

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

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

[4] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995); A. Muller, H. Zbinden, and N. Gisin, Nature **378**, 449 (1995); R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Opt. **47**, 533 (2000).

[5] 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).

[6] C. H. Bennett and G. Brassard, in *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 1984* (IEEE Press, New York, 1984), p. 175.

[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).

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

[11] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); Phys. Rev. A **72**, 012322 (2005); **72**, 049908(E) (2005).

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

[13] 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, in *Proceedings of IEEE International Symposium on Information Theory (ISIT'06), Seattle, Washington, 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, *ibid.* **98**, 010503 (2007); T. Schmitt-Manderbach *et al.*, *ibid.* **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, e-print arXiv:0705.3081 [quant-ph] (to be published); J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Opt. Express **15**, 8465 (2007).

[14] W. Mauerer and C. Silberhorn, Phys. Rev. A **75**, 050305(R) (2007).

[15] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007).

[16] X. Ma and H.-K. Lo, New J. Phys. **10**, 073018 (2008).

[17] D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, and I. A. Walmsley, Opt. Lett. **28**, 2387 (2003).

[18] M. Curty, T. Moroder, X. Ma, and N. Lütkenhaus, Opt. Lett. **34**, 3238 (2009).

[19] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, in *Proceedings 8th Asian Conference on Quantum Information Science (AQIS'08), Seoul, South Korea, 2008;* New J. Phys. **11**, 113033 (2009).

[20] H.-K. Lo, Quantum Inf. Comput. **5**, 413 (2005).

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

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

[23] M. S. Bazaraa, J. J. Jarvis, and H. D. Sherali, *Linear Programming and Network Flows* (Wiley, New York, 2004), 3rd Ed.

[24] P. P. Rohde and T. C. Ralph, J. Mod. Opt. **53**, 1589 (2006).

[25] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

[26] G. Arfken, *Mathematical Methods for Physicists* (Academic Press, New York, 1985), 3rd Ed.

[27] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables* (Dover, New York, 1972), 9th Ed.

[28] M. Hayashi, Phys. Rev. A **79**, 020303(R) (2009); C.-H. F. Fung, X. Ma, and H. F. Chau, e-print arXiv:0910.0312; X. Ma, C.-H. F. Fung, J.-C. Boileau, and H. F. Chau, e-print arXiv:0904.1994.

[29] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, 1985).