Passive decoy state quantum key distribution with practical light sources

Marcos Curty¹, Xiongfeng Ma², Bing Qi³, and Tobias Moroder²,⁴,⁵

¹ ETSI Telecommunicación, 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 3G1 Toronto, Ontario, Canada
⁴ Quantum Information Theory Group, Institute of Theoretical Physics I, University of Erlangen-Nürnberg, 91058 Erlangen, Germany
⁵ Max Planck Institute for the Science of Light, 91058 Erlangen, Germany

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. While 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 paper we extend these results, now showing specifically the analysis for other practical scenarios with different light sources and photo-detectors. In particular, we consider sources emitting thermal states, phase randomized WCP, and strong coherent light in combination with several types of photo-detectors, like, for instance, threshold photon detectors, photon number resolving detectors, and classical photo-detectors. 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.

PACS numbers:

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 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 multi-photon pulses [5]. This attack provides her with full information about the part of the key generated with the multi-photon 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 $\eta$ denotes the transmission efficiency of the quantum channel [2, 6]. 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 $\eta$.

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 [1, 11, 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 \cite{13}, which show the practical feasibility of this method.

While 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 practical implementations.

Known passive schemes rely typically on the use of a parametric down-conversion (PDC) source together with a photon detector \cite{14, 12, 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. \cite{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 \cite{17}. Ref. \cite{12} analyzes the scenario where the detector used by Alice is just a simple threshold detector, while the authors of Ref. \cite{16} generalize the ideas introduced by Mauerer et al. in Ref. \cite{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 \cite{18}. That is, one does not need a non-linear 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. \cite{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. \cite{14, 15, 16}: By measuring one of the two output signals of the BS, the conditional photon number distribution of the other signal varies depending on the result obtained \cite{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 \cite{18}. A similar result can also be obtained when Alice uses heralded single-photon sources showing non-Poissonian photon number statistics \cite{19}.

In this paper we extend the results presented in Ref. \cite{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. \cite{18}. On the other hand, PNR detectors allows us to obtain ultimate lower bounds on the maximal performance that can be expected at all from this kind 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 it can operate with a simpler classical photo-detector. This fact makes this setup specially 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 paper 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. \cite{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 paper 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 \cite{9, 10, 11, 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

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 \cite{9, 10, 11, 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
The parameter \( q \) is described as \( R \) where \( f \) for its efficient version \([21]\); the error correction protocol as a function of the error of parameters \( n \rangle \) such states can be de-
scribed as

\[
\rho^l = \sum_{n=0}^{\infty} p_n^l |n\rangle\langle n|,
\]

(1)

where \( |n\rangle \) denote Fock states with \( n \) photons.

The gain \( Q^l \) corresponding to setting \( l \), i.e., 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

\[
Q^l = \sum_{n=0}^{\infty} p_n^l Y_n,
\]

(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 \( l \), that we shall denote as \( E^l \), is given by

\[
Q^l E^l = \sum_{n=0}^{\infty} p_n^l Y_n e_n,
\]

(3)

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

In this paper we shall consider that Alice and Bob treat each decoy setting separately, and they distill se-
cret key from all of them. We use the security analysis presented in Ref. \([11]\), 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

\[
R \geq \max \{ R^l, 0 \},
\]

(4)

where \( R^l \) satisfies

\[
R^l \geq q \{ -Q^l f(E^l) H(E^l) + p_1^l Y_1[1 - H(e_1)] + p_0^l Y_0 \}.
\]

(5)

The parameter \( q \) is the efficiency of the protocol \( q = 1/2 \) for the standard BB84 protocol \([8]\), 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 \( f(E^l) \approx 1 \) 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. \( 4 \), one needs to solve Eqs. \( 2 \) - \( 3 \) 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, like, for instance, linear programming tools \([22]\), which might result in a 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 paper 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 like, for instance, stray light coming from timing pulses which are not completely filtered out in reception. In the scenario considered, the yields \( Y_n \) can be expressed as \([10, 12]\)

\[
Y_n = 1 - (1 - Y_0)(1 - \eta_{\text{sys}})^n,
\]

(6)

where \( \eta_{\text{sys}} \) represents the overall transmittance of the system. This quantity can be written as

\[
\eta_{\text{sys}} = \eta_{\text{channel}}\eta_{\text{Bob}},
\]

(7)

where \( \eta_{\text{channel}} \) is the transmittance of the quantum channel, and \( \eta_{\text{Bob}} \) denotes the overall transmittance of Bob's detection apparatus. That is, \( \eta_{\text{Bob}} \) includes the transmittance of any optical component within Bob's measurement device and the detector efficiency. The parameter \( \eta_{\text{channel}} \) can be related with a transmission distance
FIG. 1: Basic setup of a passive decoy state QKD scheme: Interference of two Fock diagonal states, $\rho$ and $\sigma$, at a beam splitter (BS) of transmittance $t$; $a$ and $b$ represent the two output modes.

$d$ measured in km for the given QKD scheme as

$$\eta_{\text{channel}} = 10^{-\frac{d}{10}} \text{dB/km},$$

where $\alpha$ 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 $\epsilon_n$ is given by $^{10, 12}$

$$\epsilon_n = \frac{Y_0 e_d + (Y_n - Y_0) e_d}{Y_n},$$

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., $\epsilon_0 = 1/2$.

**IV. PASSIVE DECOY STATE QKD SETUP**

The basic setup is rather simple $^{18}$. It is illustrated in Fig. 1. Suppose two Fock diagonal states

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

$$\sigma = \sum_{n=0}^{\infty} r_n |n\rangle \langle n|,$$

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 photo-detectors. We start by considering a simple source of thermal states. Afterwards, we investigate more practical sources of coherent light.

**V. THERMAL LIGHT**

Suppose that the signal state $\rho$ which appears in Fig. 1 is a thermal state of mean photon number $\mu$. Such state can be written as

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

and let $\sigma$ 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

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

$$p_n^t = \sum_{m=0}^{\infty} p_{n,m} = \frac{1}{1 + \mu t} \left( \frac{\mu t}{1 + \mu t} \right)^n.$$ (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) which contains two elements, $F_{\text{vac}}$ and $F_{\text{click}}$, given by $^{24}$

$$F_{\text{vac}} = (1 - \epsilon) \sum_{n=0}^{\infty} (1 - \eta_d)^n |n\rangle \langle n|,$$

$$F_{\text{click}} = \mathbb{1} - F_{\text{vac}}.$$ (14)

The parameter $\eta_d$ denotes the detection efficiency of the detector, and $\epsilon$ represents its probability of having a dark count. Eq. (14) assumes that $\epsilon$ is, to a good approximation, independent of the incoming signals. The outcome of $F_{\text{vac}}$ corresponds to “no click” in the detector, while the operator $F_{\text{click}}$ 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 $p_n^t$, has the form

$$p_n^t = (1 - \epsilon) \sum_{m=0}^{\infty} (1 - \eta_d)^m p_{n,m} = \frac{(1 - \epsilon)}{r} \left( \frac{\mu t}{r} \right)^n,$$ (15)

with the parameter $r$ given by

$$r = 1 + \mu [t + (1-t) \eta_d].$$ (16)
If the detector produces a click, the joint probability of finding \( n \) photons in mode \( a \) is given by

\[
p_c^a = p_n^a - p_n^c.
\]

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): \( q_n^c = p_n^c/(1 - N_{th}) \) and \( q_n^a = p_n^a/N_{th} \), with

\[
N_{th} = \sum_{n=0}^{\infty} p_n^c = \frac{1 - \epsilon}{1 + \mu \eta_{d}(1 - t)}.
\]

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. (3) - (5) into the gain and QBER formulas we obtain that the parameters \( Q^c \), \( E^c \), \( Q^t \), and \( E^t \) can be written as

\[
Q^c = N_{th} - \frac{(1 - \epsilon)(1 - Y_0)}{r - (1 - \eta_{sys})\mu t},
\]

\[
Q^e E^c = (e_0 - e_d)Y_0 N_{th} + e_d Q^c,
\]

\[
Q^t = \frac{Y_0}{1 + \mu \eta_{sys}},
\]

\[
Q^t E^t = (e_0 - e_d)Y_0 + e_d Q^t,
\]

where \( Q^c = Q^t - Q^e \) and \( Q^e E^c = Q^t E^t - Q^e E^c \).

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. 23: \( Y_0 = 1.7 \times 10^{-6}, e_d = 0.033, \alpha = 0.21 \text{ dB/km}, \) and Bob’s detection efficiency \( \eta_{Bob} = 0.045 \). We further assume that \( q = 1 \), and \( f(E) = f(E^c) = 1.22 \). These data are used as well for simulation purposes in the following sections. We study two different scenarios: (A) A perfect threshold detector, \( \epsilon \approx 0 \) and \( \eta_{d} = 1 \), and (B) \( \epsilon = 3.2 \times 10^{-7} \) and \( \eta_{d} = 0.12 \). In both cases we find that the values of the mean photon number \( \mu \) and the transmittance \( t \) which maximize the secret key rate formula are quite similar and almost constant with the distance. In particular, \( \mu \) 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 times. 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 \( q_n^c \) satisfy \( q_0^c \approx 1 \) and \( q_{n \geq 1}^c \approx 0 \). 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 into an enhancement of the achievable secret key rate and distance. The cutoff point where the secret key rate drops down to zero is \( l \approx 126 \text{ km} \).

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 illustrates also 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 at all with such an scheme and the security analysis provided in Refs. [3, 20].

VI. WEAK COHERENT LIGHT

Suppose now that the signal states \( \rho \) and \( \sigma \) which appear in Fig. 1 are two phase randomized WCP emitted by a pulsed laser source. That is,

\[
\rho = e^{-\mu_1} \sum_{n=0}^{\infty} \frac{\mu_1^n}{n!} |n\rangle \langle n|,
\]

\[
\sigma = e^{-\mu_2} \sum_{n=0}^{\infty} \frac{\mu_2^n}{n!} |n\rangle \langle n|,
\]

(20)

with \( \mu_1 \) and \( \mu_2 \) 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]

\[
p_{n,m} = \frac{\nu^{n+m}e^{-\nu}}{n!m!} \frac{1}{2\pi} \int_{0}^{2\pi} \gamma^n(1-\gamma)^m d\theta,
\]

(21)

where the parameters \( \nu, \gamma, \) and \( \xi, \) are given by

\[
\nu = \mu_1 + \mu_2,
\]

\[
\gamma = \frac{\mu_1 t + \mu_2(1-t) + \xi \cos \theta}{\nu},
\]

\[
\xi = 2\sqrt{\mu_1\mu_2(1-t)t}.
\]

(22)

This result differs from the one expected from the interference of two pure coherent states with fixed phase relation, \( |\sqrt{\mu_1}e^{i\phi_1}| \) and \( |\sqrt{\mu_2}e^{i\phi_2}| \), 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

\[
p_n^a = \sum_{m=0}^{\infty} p_{n,m} = \frac{\nu^n}{n!} \frac{1}{2\pi} \int_{0}^{2\pi} \gamma^n e^{-\nu\gamma} d\theta,
\]

(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. VA. In particular, the joint probability for seeing \( n \) photons in mode \( a \) and no click in the threshold detector has now the form

\[
p_n^\ddag = (1 - \epsilon) \sum_{m=0}^{\infty} (1 - \eta_l)^m p_{n,m}
\]

(24)

\[
= (1 - \epsilon) \frac{\nu^n e^{-\eta_l\nu}}{n!} \frac{1}{2\pi} \int_{0}^{2\pi} \gamma^n e^{-(1-\eta_l)\nu\gamma} d\theta.
\]

On the other hand, if the detector produces a click, the joint probability of finding \( n \) photons in mode \( a \) depending on the result of the detector (click and no click): \( q_n^c = p_n^c/(1 - N_w) \) and \( q_n^e = p_n^e/N_w \), with

\[
N_w = \sum_{n=0}^{\infty} p_n^\ddag = (1 - \epsilon) e^{-\eta_l[\mu_1(1-t) + \mu_2 t]} I_0,\nu_l,\xi,
\]

(25)

and where \( I_{\nu,z} \) represents the modified Bessel function of the first kind [20]. This function is defined as [20]

\[
I_{\nu,z} = \frac{1}{2\pi i} \int e^{(z/2)(t+1/t)} t^{\nu-1} dt.
\]

(26)

Figure 4 includes as well a comparison between \( q_n^e \) and a Poissonian distribution of the same mean photon number (Cases C and D). Both distributions, \( q_n^e \) and \( q_n^d \), are also non-Poissonian.
B. Lower bound on the secret key rate

To apply the secret key rate formula given by Eq. (5), with \( l \in \{c, e\} \), 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 \( p_{l_0}^c \) and \( p_{l_1}^e \) 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 \( p_{l_0}^c \) and \( p_{l_1}^e \), with \( n = 0, 1, 2 \). These probabilities can be obtained by solving Eqs. (23)-(24). They are given in Appendix C. Note that \( p_{l_{0 12}}^c \) can be directly calculated from these two statistics by means of Eq. (17). After substituting Eqs. (B7)-(B9) into the gain and QBER formulas we obtain

\[
Q^E = N_w - (1 - \epsilon)(1 - Y_0)e^{(\eta_d - \eta_{sys})w - \eta_{sys}t} \\
Q^E = N_w + e_dQ^E, \\
Q^t = 1 - (1 - Y_0)e^{-\eta_{sys}w}I_0, \\
Q^t = (e_0 - e_d)Y_0 + e_dQ^t,
\]

with the parameter \( \omega \) given by

\[
\omega = \mu_1 t + \mu_2(1 - t).
\]

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: (A) \( \epsilon = 0 \) and \( \eta_d = 1 \) [18], and (B) \( \epsilon = 3.2 \times 10^{-7} \) and \( \eta_d = 0.12 \) [22]. In both cases the optimal values of the intensities \( \mu_1 \) and \( \mu_2 \) 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 \( \mu_1 \) and \( \mu_2 \) 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 situation might not be optimal. Specially, since in this scenario the two output distributions \( p_{0 12}^c \) and \( p_{0 12}^e \) might be too close to each other for being distinguished in practice. This effect could be specially 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 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.

Like 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 B. The result is also shown in Fig. 5. It reproduces approximately the behavior of the asymptotic active setup and the secret key rate is 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. (18) 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. (18), 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 employs two independent sources of signal states. This fact might become specially relevant when she uses phase randomized WCP, since in this situation none of the signal states entering the BS can be the vacuum state.

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 \( \rho \) and \( \sigma \) are two phase randomized WCP given by Eq. (20). The transmittance of the BS is \( t = 1/2 \). We consider two possible scenarios: (A) \( \epsilon = 0 \) and \( \eta_d = 1 \) [18] (i.e., a perfect threshold photon detector), and (B) \( \epsilon = 3.2 \times 10^{-7} \) and \( \eta_d = 0.12 \) [22]. 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 B), and the secret key rate is both scenarios cannot be distinguished with the resolution of this figure.
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. 2. This setup has only one laser diode, but follows a similar spirit like the original scheme in Fig. 1, where a photo-detector 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 optical 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 product of mixtures of Fock states. Then, one can directly apply the security analysis provided in Refs. 8, 11, 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. 1 and Fig. 2 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.

\section{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 $\rho$ and $\sigma$ is now very high; for instance, approximately $10^8$ photons. This fact allows Alice to use a simple classical photo-detector 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 $\rho$ and $\sigma$, 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 $\rho$ ($\sigma$), and let $I_a(\theta)$ [$I_b(\theta)$] be the intensity of the output pulses in mode $a$ ($b$). Here the angle $\theta$ is just a function of the relative phase between the two input states. It is given by

$$\theta = \phi_1 - \phi_2 + \pi/2,$$

where $\phi_1$ ($\phi_2$) denotes the phase of the signal $\rho$ ($\sigma$). Like in Sec. VI, we assume that these phases are uniformly distributed between $0$ and $2\pi$ for each pair of input states. This can be achieved, for instance, if Alice uses two pulsed laser sources to prepare the signals $\rho$ and $\sigma$. With this notation, we have that $I_a(\theta)$ and $I_b(\theta)$ can be expressed as

$$I_a(\theta) = t_1 I_1 + r_1 I_2 + 2 \sqrt{I_1 r_1 I_2} \cos \theta,$$

$$I_b(\theta) = r_1 I_1 + t_1 I_2 - 2 \sqrt{I_1 r_1 I_2} \cos \theta,$$

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

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

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

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

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

$$
\begin{align*}
p_n^{<I_M} &= \frac{t_2^n}{n!} \int_{0}^{\theta_{th}} I_a(\theta)^n e^{-I_a(\theta) t_2} d\theta. (33)
\end{align*}
$$

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

$$
\begin{align*}
p_n^{>I_M} &= \frac{1}{n!} \int_{0}^{\pi} I_a(\theta)^n e^{-I_a(\theta) t_2} d\theta. (34)
\end{align*}
$$

Figure 3 (Case 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 $I_M$): $q_n^{<I_M} = p_n^{<I_M}/N_s$ and $q_n^{>I_M} = p_n^{>I_M}/(1-N_s)$, with

$$
N_s = \sum_{n=0}^{\infty} p_n^{<I_M} = \frac{\theta_{th}}{\pi}. (35)
$$

This figure includes as well a comparison between $q_n^{<I_M}$ (Case B) and $q_n^{>I_M}$ (Case 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.

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 $\epsilon_1$. 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 $\theta_{th} = \pi/2$. The relevant statistics $p_n^{<I_M}$ and $p_n^{>I_M}$, with $n = 0, 1, 2$, are calculated in Appendix B. After substituting Eqs. (B6)-(B9) into the gain and QBER formulas we obtain

$$
\begin{align*}
Q^{<I_M} &= N_s - \frac{1}{2} \left( 1 - Y_0 \right) e^{-\eta_{sys} \kappa} (I_{0,\eta_{sys} \kappa} - L_{0,\eta_{sys} \kappa}), \\
Q^{<I_M} E^{<I_M} &= (e_0 - e_d) Y_0 N_s + e_d Q^{<I_M}, \\
Q^{>I_M} &= (1 - N_s) - \frac{1}{2} \left( 1 - Y_0 \right) e^{-\eta_{sys} \kappa} \\
&\times (I_{0,\eta_{sys} \kappa} + L_{0,\eta_{sys} \kappa}), \\
Q^{>I_M} E^{>I_M} &= (e_0 - e_d) Y_0 (1 - N_s) + e_d Q^{>I_M}, (36)
\end{align*}
$$

where the parameter $\kappa$ is given by

$$
\kappa = I t_2, (37)
$$

and $L_{q,z}$ represents the modified Struve function defined by Eq. (142).

The resulting lower bound on the secret key rate is illustrated in Fig. 10. We study two different situations: (A) We impose $t_1 = 1/2$, i.e., we consider a simple 50 : 50
FIG. 10: Lower bound on the secret key rate $R$ given by Eq. (3) in logarithmic scale for the passive decoy state setup illustrated in Fig. 4 with two intensity settings. We consider two possible scenarios: (A) We impose $t_1 = 1/2$, i.e., we consider a simple 50 : 50 BS, and we optimize the parameter $\kappa$ (dashed line), and (B) we optimize both parameters, $t_1$ and $\kappa$ (solid line).

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 $c$.

have 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 like in Sec. VII C and we omit it for simplicity. The resulting secret key rate in the active scheme is half the one of the passive setup.

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 which are measured in the experiment each fluctuates around its asymptotic value.

Our main objective here is to obtain a lower bound on the secret key rate formula given by Eq. (3) 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 which 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. VII C. Note, however, that a similar analysis can also be applied to the other passive schemes presented in this paper.

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

$$Y_1 \geq Y_1^L = \frac{\mu^2 Q_\nu e^\nu - \nu^2 Q_\mu e^\mu - (\mu^2 - \nu^2) Y_0}{\mu \nu (\mu - \nu)}$$

$$e_1 \leq e_1^U = \frac{E_\mu Q_\nu e^\nu - e_0 Y_0}{Y_1^U \mu},$$

(38)
where $\mu$ ($\nu$) denotes the mean photon number of a signal (decoy) state, $Q_\mu$ ($Q_\nu$) and $E_\mu$ ($E_\nu$) 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

\[ Q_\mu = Y_0 + 1 - e^{-\mu_{\text{sys}}}, \]
\[ E_\mu Q_\mu = e_\mu Y_0 + e_d (1 - e^{-\mu_{\text{sys}}}), \]
\[ Q_\nu = Y_0 + 1 - e^{-\nu_{\text{sys}}}, \]
\[ E_\nu Q_\nu = e_\nu Y_0 + e_d (1 - e^{-\nu_{\text{sys}}}). \]  

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

\[ \Delta Q_\mu = u_\alpha \sqrt{Q_\mu / N_\mu}, \]
\[ \Delta Q_\nu = u_\alpha \sqrt{Q_\nu / N_\nu}, \]
\[ \Delta Q_\mu E_\mu = u_\alpha \sqrt{2E_\mu Q_\mu / N_\mu}, \]
\[ \Delta Q_\nu E_\nu = u_\alpha \sqrt{2E_\nu Q_\nu / N_\nu}, \]  

where $N_\mu$ ($N_\nu$) denotes the number of signal (weak decoy) pulses sent by Alice, and $u_\alpha$ represents the number 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 which 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 $e_1$ which do not depend on $Y_0$. Specifically, from Eqs. (2)-(3) we obtain that

\[ (1 - 2e_1)Y_1 \geq A = \frac{\mu}{\nu(\mu - \nu)} Q_\nu (1 - 2E_\nu) e_\nu \]
\[ - \frac{\nu}{\mu(\mu - \nu)} Q_\mu (1 - 2E_\mu) e_\mu. \]  

The gains $Q_\mu$ and $Q_\nu$, together with the QBERs $E_\mu$ and $E_\nu$, are directly measured in the experiment, and their statistical fluctuations are given by Eq. (40). On the other hand, we have that

\[ e_1 \leq \frac{B}{Y_1^{\frac{1}{2}}}, \]  

with the parameter $B$ given by

\[ B = \min \left\{ \frac{E_\nu Q_\nu e_\nu}{\nu}, \frac{E_\mu Q_\mu e_\mu - E_\nu Q_\nu e_\nu}{\mu - \nu} \right\}. \]  

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

\[ Y_1 [1 - H(e_1)] \geq A \frac{1}{1 - 2e_1} \left[ 1 - H\left( \frac{B(1 - 2e_1)}{A} \right) \right]. \]

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. (4) 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

\[ Y_1^U = A + 2B, \]
\[ e_1^U = \frac{B}{A + 2B}, \]  

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

\[ \Delta_A = (c_1 \Delta Q_\nu)^2 + 4(c_1 \Delta E_\nu Q_\nu)^2 + (c_2 \Delta Q_\mu)^2 \]
\[ + 4(c_2 \Delta E_\mu Q_\mu)^2 \frac{1}{2}, \]
\[ \Delta_B = \min \left\{ \frac{e_\mu \Delta E_\mu Q_\mu}{\mu}, \frac{e_\nu \Delta E_\nu Q_\nu}{\nu}, \right. \]
\[ \left. \frac{\sqrt{(e_\mu \Delta E_\mu Q_\mu)^2 + (e_\nu \Delta E_\nu Q_\nu)^2}}{\mu - \nu} \right\}, \]  

where the coefficients $c_1$ and $c_2$ have the form

\[ c_1 = \frac{\mu}{\nu(\mu - \nu)} e_\nu, \]
\[ c_2 = \frac{\nu}{\mu(\mu - \nu)} e_\mu, \]

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

\[ \Delta Y_1 [1 - H_2(e_1)] = \left\{ \Delta_A \log_2 \left( \frac{2A + 2B}{A + 2B} \right) \right\}^2 \]
\[ + \left\{ \Delta_B \log_2 \left( \frac{4B(A + B)}{(A + 2B)^2} \right) \right\}^2 \frac{1}{2}. \]
The result is illustrated in Fig. 12 (dashed line). Here we consider four possible scenarios: (A) An active decoy state setup (with only one decoy state) with statistical fluctuations (dashed line) [12]. (B) An active decoy state setup (with only one decoy state) without considering statistical fluctuations (thick solid line) [12], (C) The passive decoy state scheme with WCP introduced in Sec. VI with 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 $B$ are now given by

\[
A = \frac{\bar{p}_{\eta} Q^t(1 - 2 E^t) - \bar{p}_{\eta} Q^e(1 - 2 E^e)}{p_2 p_1 - \bar{p}_{\eta} p_1},
\]

\[
B = \min \left\{ \frac{E^t Q^e}{p_1}, \frac{p_6 E^t Q^e - p_6 E^e Q^e}{p_1 p_1 - \bar{p}_{\eta} p_1} \right\},
\]

while Eq. (43) is still valid in this scenario. The deviations of $A$ and $B$ have the form

\[
\Delta_A = \frac{1}{p_2 p_1 - \bar{p}_{\eta} p_1} \left[ (\bar{p}_{\eta} \Delta Q^t)^2 + 4 (\bar{p}_{\eta} \Delta E^t Q^t)^2 \right. + (\bar{p}_{\eta} \Delta Q^e)^2 + 4 (\bar{p}_{\eta} \Delta E^e Q^e)^2 \right]^{1/2},
\]

\[
\Delta_B = \min \left\{ \frac{\Delta E^t Q^t}{p_1}, \frac{\Delta E^e Q^e}{p_1}, \frac{\sqrt{(p_6 \Delta E^t Q^t)^2 + (p_6 \Delta E^e Q^e)^2}}{p_6 p_1 - \bar{p}_{\eta} p_1} \right\}.
\]

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

\[
\Delta Q^t = u_{\alpha} \sqrt{Q^t/N},
\]

\[
\Delta Q^e = u_{\alpha} \sqrt{Q^e/N},
\]

\[
\Delta E^t Q^t = u_{\alpha} \sqrt{E^t Q^t / N},
\]

\[
\Delta E^e Q^e = u_{\alpha} \sqrt{E^e Q^e / N},
\]

where $N^e$ 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 $Y_1[1 - H_2(\epsilon_1)]$ is again given by Eq. (43).

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 the one of the previous section, i.e., $N = 6 \times 10^9$. We study two different situations depending on the efficiency of Alice’s threshold detector: $\eta_d = 1$ (thin solid line), and $\eta_d = 0.4$ (dash-dotted line). In both cases the optimal values of the intensities $\mu_1$ and $\mu_2$ 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.
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 $\eta_l$. 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 specially 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 paper we have extended the results presented in Ref. [15], 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 (PNR) detectors. In the case of threshold detectors, we have included as well the effect that detection inefficiencies and dark counts present in current photodetectors, but it can operate with a simpler classical photo-detector. This fact makes this setup especially 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.

X. ACKNOWLEDGEMENTS

The authors wish to 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 NSERC 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. 9. This expression can be lower bounded by

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

where $e_1^l$ 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 $e_1^l$. 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. VI.

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

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

$$p_1^l Y_1 + p_0^l Y_0 \geq p_1^l Y_1^L + p_0^l Y_0, \quad (A2)$$

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

$$p_2^l Q^l - p_2^l Q^l = \sum_{n=0}^{\infty} (p_2^l Y_1 - p_2^l Y_0) Y_n \leq \sum_{n=0}^{1} (p_2^l Y_1 - p_2^l Y_0) Y_n, \quad (A3)$$

since

$$p_2^l Y_1 - p_2^l Y_0 = \frac{(1 - \epsilon)(\mu\eta)^n \epsilon^{n+2}}{(1 + \mu)(1 + \mu\eta)^n} \leq \frac{1}{1 + \mu \eta} \leq 0, \quad (A4)$$

for all $n \geq 2$, and where the parameter $r$ is given by Eq. 10. To see this, note that the first term on the r.h.s. of Eq. [A3] is always greater or equal than zero, and $r \geq 1 + \mu \eta \geq 1$. Similarly, we have that $p_2^l Y_1 - p_2^l Y_0 \geq 0$ for all $n \leq 1$. Combining both results, we obtain

$$Y_1 \geq Y_1^L = \max \left\{ \frac{p_2^l Q^l - p_2^l Q^l - (p_2^l Y_0 - p_2^l Y_0) Y_0}{p_2^l Y_1 - p_2^l Y_0}, 0 \right\}. \quad (A5)$$

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

$$- p_1^l \left( p_2^l Y_1 - p_2^l Y_0 \right) \leq \left( p_2^l p_0^l - p_2^l p_1^l \right) Y_0 \leq 0. \quad (A6)$$

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

$$p_0^l \left( p_2^l p_0^l - p_2^l p_1^l \right) \leq p_1^l \left( p_2^l p_0^l - p_2^l p_1^l \right). \quad (A7)$$
since, as we have seen above, \( p^c_n p^c_\bar{n} - p^c_\bar{n} p^c_n \geq 0 \). After a short calculation, it turns out that Eq. (A7) can be further simplified to
\[
\frac{p^t_1 p^t_n - p^t_\bar{n} p^t_n}{p^t_\bar{n} p^t_n} \geq 0, \tag{A8}
\]
both for \( l = c \) and \( l = \bar{c} \). Finally, from the definition of the probabilities \( p^t_n \) and \( p^t_\bar{n} \) given by Eqs. (13)-(15), we find that
\[
p^t_1 p^\tilde{n}_n - p^t_\bar{n} p^\tilde{n}_n = \frac{(1 - \epsilon)(\mu t)^{n+1}}{[(1 + \mu t)^{r-1}]} \times \left( \frac{1}{r^{n-1}} - \frac{1}{(1 + \mu t)^{n-1}} \right), \tag{A9}
\]
which is greater or equal than zero for all \( n \leq 1 \), and negative otherwise. Note that the first term on the r.h.s. of Eq. (A9) is always greater or equal than zero, and the sign of the second term depends on the value of \( n \), since \( r \geq 1 + \mu t \geq 1 \).

We obtain, therefore, that
\[
P^t_1 Y_1 + p^t_0 Y_0 \geq \max \left\{ \left( p^t_1 p^\tilde{Q}_n - p^t_\bar{n} p^\tilde{Q}_n \right) \right\}
\]
\[
+ \left[ \left( p^t_0 p^\tilde{Q}_n - p^t_\bar{n} p^\tilde{Q}_n \right) \right] Y^u_0, \tag{A10}
\]
for all \( l \in \{c, \bar{c}\} \), and where \( Y^u_0 \) denotes an upper bound on the background rate \( Y_0 \). This parameter can be calculated from Eq. (3). In particular, we have that
\[
Q^\tilde{e} E^c = \sum_{n=0}^{\infty} p^\tilde{e}_n Y_n e_n \geq p^\tilde{e}_0 Y_0 e_0, \tag{A11}
\]
and similarly for the product \( Q^\bar{e} E^c \). We find
\[
Y_0 \leq Y^u_0 = \min \left\{ \frac{E^c Q^\tilde{e}}{p^\tilde{e}_0} \right\} \frac{E^c Q^\bar{e}}{p^\bar{e}_0} e_0. \tag{A12}
\]

2. Upper bound on \( e_1 \)

For this, we proceed as follows:
\[
p_0 Y_0 - p^\tilde{Q}_n Y_n e_n \geq \sum_{n=1}^{\infty} (p^t_1 p^\tilde{Q}_n - p^t_\bar{n} p^\tilde{Q}_n) Y_1 e_1, \tag{A13}
\]
where the inequality condition comes from the fact that
\[
p^t_1 p^\tilde{n}_n - p^t_\bar{n} p^\tilde{n}_n = \frac{(1 - \epsilon)(\mu t)^n}{(1 + \mu t)^r} \frac{1}{r^n} \geq 0, \tag{A14}
\]
for all \( n \geq 1 \). From Eq. (A13) we obtain, therefore, that \( e_1 \) is upper bounded by \( \frac{p^\tilde{e}_0 Y_0}{(p^\tilde{e}_0 Y_0 - p_0 Y_0) Y_1 e_1} \), where \( Y_1 e_1 \) is given by Eq. (A5) with the parameter \( Y_0 \) replaced by \( Y^u_0 \).

On the other hand, note that Eq. (3) also provides a simple upper bound on \( e_1 \). Specifically,
\[
Q^\tilde{e} E^c = \sum_{n=0}^{\infty} p^\tilde{e}_n Y_n e_n \geq p^\tilde{e}_0 Y_0 e_0 + p^\tilde{e}_1 Y_1 e_1. \tag{A15}
\]
and similarly for the product \( Q^\bar{e} E^c \). Putting all these conditions together, we find that
\[
e_1 \leq e_1 U = \min \left\{ \frac{E^c Q^\tilde{e}}{p^\tilde{e}_1 Y_1 e_1} \right\} \frac{E^c Q^\bar{e}}{p^\bar{e}_1 Y_1 e_1}, \tag{A16}
\]
where \( Y^u_0 \) represents a lower bound on the background rate \( Y_0 \). To calculate this parameter we use the following inequality:
\[
p_0 Y_0 - p^\tilde{Q}_n Y_n e_n \geq \sum_{n=2}^{\infty} (p^t_1 p^\tilde{Q}_n - p^t_\bar{n} p^\tilde{Q}_n) Y_0 e_0 \geq (p^t_1 p^\tilde{Q}_n - p^t_\bar{n} p^\tilde{Q}_n) Y_0 e_0, \tag{A17}
\]
where, as we have seen above, \( p^t_1 p^\tilde{Q}_n - p^t_\bar{n} p^\tilde{Q}_n \leq 0 \) for all \( n \geq 2 \). From Eq. (A17) we obtain, therefore, that
\[
Y_0 \geq Y^u_0 = \max \left\{ \frac{p^\tilde{Q}^c - p^\bar{Q}^c}{p^\tilde{e}_0 Y_0 - p^\bar{e}_0 Y_0}, 0 \right\}. \tag{A18}
\]

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 at all with the passive decoy state setups introduced in Sec. IV and Sec. V in combination with the security analysis provided in Refs. 8, 20.

A perfect PNR detector can be characterized by a POVM which 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. IV 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: $p_{n,m}^a = p_{n,m}/N_m$, with

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

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 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

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

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

$$X_m = \sum_{n=0}^{\infty} \binom{n + m}{m} V_n. \quad (B4)$$

That is, the coefficient matrix of the system of linear equations given by Eq. 13 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. 13. 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. 14-17 into the gain and QBER formulas we obtain

$$Q^m = N_m - \frac{(1 - Y_0)[\mu(1-t)]^m}{(1 + \mu)[1 - (1 - \eta_{sys})t]} \left[ \frac{\mu}{1 + \mu} \right]^{m+1},$$
$$Q^m E^m = (e_0 - e_d)Y_0N_m + e_dQ^m. \quad (B5)$$

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

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

The resulting lower bound on the secret key rate is illustrated in Fig. 13 (solid line). The optimal values of the parameters $\mu$ and $t$ are quite constant with the distance. Specifically, in this figure we choose $\mu$ around 18.5 and $t$ around 0.02.

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 $m$ 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: $p_{n,m}^a = p_{n,m}/N_m$, with

$$N_m = \sum_{n=0}^{\infty} p_{n,m} = \frac{e_0 e^{-v}}{m!} \frac{1}{2\pi} \int_0^{2\pi} (1 - \gamma)^m e^{i\gamma} d\theta. \quad (B7)$$

To show that the experimental observations associated to 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 B 1. That is, one could try to prove that the determinant of the coefficient matrices associated to the systems of linear equations given by Eqs. 14-17 is different from zero also in this scenario. For simplicity, here we have confirmed this statement only numerically.

After substituting Eqs. 14-17 into the gain and QBER
formulas we obtain

\[ Q^m = \frac{\nu^m e^{-\nu}}{m!} \int_0^{2\pi} \frac{1}{2\pi} e^{-(1-Y_0)e^{-\eta_0\nu \gamma}} \times (1-\gamma)^m e^{\nu \gamma} d\theta, \]

\[ Q^m E^n = (e_0-e_d)Y_0 N_m + e_d Q^m. \]  

(B8)

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

\[ p_{0,m} = e^{-\nu(v-\omega)m} g \left[ \frac{1-m}{2}, \frac{m}{2}, 1, (v-\omega)^2 \right], \]

\[ p_{1,m} = \omega p_{0,m} \frac{e^{-\nu \xi^2}}{2T_m} \times g \left[ \frac{1-m}{2}, 1, \frac{m}{2}, 2, (v-\omega)^2 \right], \]  

(B9)

where the Gamma function \( \Gamma_z \) is defined as

\[ \Gamma_z = \int_0^\infty t^{z-1} e^{-t} dt, \]

and where \( g(a,b,c,z) \) represents the hypergeometric function. This function is defined as

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

(B10)

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 \( \mu_1 \) and \( \mu_2 \) which optimize the secret key rate formula are, respectively, \( \approx 10^{-4} \) and \( \approx 0.95 \). 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. While in the passive scheme the relevant statistics are given by the asymptotic active decoy state setup with phase randomized FCP, after a short calculation, we find that

\[ p_0^I = I_0 e^{-\omega}, \]

\[ p_1^I = (\omega I_0 e^{-\omega}), \]

\[ p_2^I = \frac{1}{2} \left[ \omega^2 I_0 + (1-2\omega)\xi I_1, \xi + \xi I_2, \xi \right] e^{-\omega}, \]  

(C1)

with \( \omega = \mu_1 + \mu_2 (1-t) \). The probabilities \( p_n^I \) have the form

\[ p_n^I = \tau I_0, (1-n_0) \xi, \]

\[ p_1^I = \tau (\omega I_0, (1-n_0) \xi - \xi I_1, (1-n_0) \xi), \]

\[ p_2^I = \tau^2 \left[ \omega^2 I_0, (1-n_0) \xi + \frac{1}{2} \left( 1-\eta_d - 2\omega \right) \xi I_1, (1-n_0) \xi \right. \]

\[ + \left. \xi I_2, (1-n_0) \xi \right], \]  

(C2)

where \( \tau = (1-\epsilon) e^{-[\eta_d v + (1-n_0)\omega]} \).

**APPENDIX D: PROBABILITIES \( p_n^{\leq I_M} \) AND \( p_n^{> I_M} \)**

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

\[ p_0^{< I_M} = \frac{e^{-\kappa}}{2} \left( I_{0, \xi} - L_0, \xi \right), \]

(D1)

\[ p_1^{< I_M} = \frac{e^{-\kappa}}{2} \left[ \kappa (I_{0, \xi} - L_0, \xi) - \zeta (I_{1, \xi} - L_{-1, \xi}) \right], \]

\[ p_2^{< I_M} = \frac{e^{-\kappa}}{4} \left\{ \kappa^2 (I_{0, \xi} - L_0, \xi) + \zeta \left[ \frac{2}{\pi} \left( 1 - \frac{\zeta^2}{3} \right) \right. \right. \]

\[ + \left. \left. (1-2\kappa) (I_{1, \xi} - L_{-1, \xi}) + \zeta (I_{2, \xi} - L_{-2, \xi}) \right] \right\}, \]  

where \( \kappa = I_{L_2}, \xi = 2\kappa \sqrt{I_{T_1}} \), and \( L_{q,z} \) represents the modified Struve function. This function is defined as

\[ L_{q,z} = \frac{z^q}{2^{q-1} \sqrt{\pi q} q^{1/2}} \int_0^{\pi/2} \sin (z \cos \theta) \sin \theta^q d\theta. \]  

(D2)

On the other hand, the probabilities \( p_n^{> I_M} \) have the form

\[ p_0^{> I_M} = \frac{e^{-\kappa}}{2} (I_{0, \xi} + L_0, \xi), \]

(D3)

\[ p_1^{> I_M} = \frac{e^{-\kappa}}{2} \left[ \kappa (I_{0, \xi} + L_0, \xi) - \zeta (I_{1, \xi} + L_{-1, \xi}) \right], \]

\[ p_2^{> I_M} = \frac{e^{-\kappa}}{4} \left\{ \kappa^2 (I_{0, \xi} + L_0, \xi) + \zeta \left[ -\frac{2}{\pi} \left( 1 - \frac{\zeta^2}{3} \right) \right. \right. \]

\[ + \left. \left. (1-2\kappa) (I_{1, \xi} + L_{-1, \xi}) + \zeta (I_{2, \xi} + L_{-2, \xi}) \right] \right\}. \]
