Entropy **2015**, *17*, 4064-4082; doi:10.3390/e17064064

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Passive Decoy-State Quantum Key Distribution with Coherent Light

Marcos Curty [1,*], Marc Jofre [2], Valerio Pruneri [2,3] and Morgan W. Mitchell [2]

[1] Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Campus Universitario, Vigo 36310, Pontevedra, Spain

[2] ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, Castelldefels 08860, Barcelona, Spain; E-Mails: marc.jofre@icfo.es (M.J.); valerio.pruneri@icfo.es (V.P.); morgan.mitchell@icfo.es (M.W.M.)

[3] ICREA-Institució Catalana de Recerca i Estudis Avançats, Barcelona 08010, Spain

* Author to whom correspondence should be addressed; E-Mail: mcurty@com.uvigo.es; Tel.: +34-986-818615.

Received: 31 March 2015 / Accepted: 9 June 2015 / Published: 12 June 2015

Abstract: Signal state preparation in quantum key distribution schemes can be realized using either an active or a passive source. Passive sources might be valuable in some scenarios; for instance, in those experimental setups operating at high transmission rates, since no externally driven element is required. Typical passive transmitters involve parametric down-conversion. More recently, it has been shown that phase-randomized coherent pulses also allow passive generation of decoy states and Bennett–Brassard 1984 (BB84) polarization signals, though the combination of both setups in a single passive source is cumbersome. In this paper, we present a complete passive transmitter that prepares decoy-state BB84 signals using coherent light. Our method employs sum-frequency generation together with linear optical components and classical photodetectors. In the asymptotic limit of an infinite long experiment, the resulting secret key rate (per pulse) is comparable to the one delivered by an active decoy-state BB84 setup with an infinite number of decoy settings.

Keywords: quantum cryptography; quantum key distribution; quantum communication

1. Introduction

Quantum key distribution (QKD) is already a mature technology that can provide cryptographic systems with an unprecedented level of security [1,2]. It aims at the distribution of a secret key between two distant parties (typically called Alice and Bob) despite the technological power of an eavesdropper (Eve) who interferes with the signals. This secret key is the essential ingredient of the one-time-pad or Vernam cipher [3], the only known encryption method that can offer information-theoretic secure communications.

Most practical long-distance implementations of QKD are based on the so-called Bennett–Brassard 1984 (BB84) protocol, introduced by Bennett and Brassard in 1984 [4], in combination with the decoy-state method [5–18]. In a typical quantum optical implementation of this scheme, Alice sends to Bob phase-randomized weak coherent pulses (WCPs) with different mean photon numbers that are selected, independently and randomly, for each signal. These states can be generated using a standard semiconductor laser together with a variable optical attenuator that is controlled by a random number generator (RNG) [19–23]. Each light pulse may be prepared in a different polarization state, which is selected, again independently and randomly for each signal, between two mutually unbiased bases, e.g., either a linear (H [horizontal] or V [vertical]) or a circular (L [left] or R [right]) polarizations basis. For simplicity, we will first consider the case of polarization encoding. Later in this paper, we will also examine phase encoding. For that, two main experimental configurations are typically used. In the first one, Alice employs four laser diodes, one for each possible BB84 signal [24,25]. These lasers are controlled by a RNG that decides each given time which one of the four diodes is triggered. The second configuration utilizes only one laser diode in combination with a polarization modulator [26–30]. This modulator rotates the state of polarization of the signals depending on the output of a RNG. On the receiving side, Bob measures each incoming signal by choosing at random between two polarization analyzers, one for each possible basis. Once the quantum communication phase of the protocol is completed, Alice and Bob use an authenticated public channel to process their data and obtain a secure secret key. Importantly, the security of decoy-state QKD has been obtained both in the asymptotic regime [6,7] and in the case of finite-length keys [31,32].

Alternatively to the active signal state preparation methods described above, Alice may as well employ a passive transmitter to generate decoy-state BB84 signals. This last solution might be desirable in some scenarios; for instance, in those experimental setups operating at high transmission rates, since no RNGs are required in a passive device [33–41]. Passive schemes might also be more robust against certain side-channel attacks hidden in the imperfections of some optical components like, for example, optical modulators used in the active sources. If a polarization modulator (or an amplitude or phase modulator) is not properly designed, for example, it may distort some of the physical parameters of the pulses emitted by the sender depending on the particular value of the polarization setting selected. This fact could open a security loophole in the active schemes.

The working principle of a passive transmitter is rather simple. For example, Alice can use various light sources to produce different signal states that are sent through an optics network. Depending on the particular detection pattern observed in some properly located photodetectors, she can infer which signal states are actually generated. Known passive schemes rely typically on the use of a parametric

down-conversion (PDC) source, where Alice and Bob passively and randomly choose which bases to measure each incoming pulse by means of a beamsplitter (BS) [40,41]. Also, Alice can exploit the photon number correlations that exist between the two output modes of a PDC source to passively generate decoy states [34]. More recently, it has been shown that phase-randomized coherent pulses are also suitable for passive preparation of decoy states [37,38] and BB84 polarization signals [42], though the combination of both setups in a single passive source is cumbersome. Intuitively speaking, Refs. [37,38,42] take advantage of the random phase of the different generated pulses to passively prepare states with either distinct photon number statistics but with the same polarization [37,38], or with different polarizations but equal intensities [42]. The preparation of phase-randomized coherent pulses could be achieved, for instance, by strongly modulating the laser diode, taking it below and above threshold [21,22].

In this article, we present a complete passive decoy-state QKD transmitter with coherent light. It shows that it is indeed possible to do state preparation for QKD in an entirely passive way using coherent states, even for BB84 signals in combination with decoy levels. Our method employs sum-frequency generation (SFG) [43–46] together with linear optical components and classical photodetectors. SFG has already exhibited its usefulness in quantum information [47–52] and device-independent QKD [53] at the single-photon level. Here we use it in the conventional non-linear optics paradigm with strong coherent light. This fact might render our proposal particularly valuable from an experimental point of view. In the asymptotic limit of an infinite long experiment, it turns out that the secret key rate (per pulse) provided by such passive scheme is similar to the one delivered by an active decoy-state BB84 setup with infinite decoy settings. Let us emphasize, however, that it is uncertain whether in practice such passive scheme could beat active transmitters or passive solutions based on a PDC source in high-speed QKD in general. Importantly, the answer will depend on various technologies.

The paper is organized as follows. In Section 2 we introduce a passive transmitter that generates decoy-state BB84 polarization signals using coherent light. Then, in Section 3 we evaluate its performance and we obtain a lower bound on the resulting secret key rate in the asymptotic regime. In Section 4 we consider the case where Alice and Bob use phase-encoding, which is more suitable to employ in combination with optical fibers than polarization encoding. Finally, Section 5 concludes the article with a summary. The paper includes as well some Appendixes with additional calculations.

2. Passive Decoy-State BB84 Transmitter

The basic setup is illustrated in Figure 1.

Let us start considering, for simplicity, the interference of two pure coherent states of frequency w_1, both prepared in $+45^\circ$ linear polarization and with arbitrary phase relationship, $|\sqrt{2\mu}e^{i\theta_1}\rangle_{a_0,+45^\circ}$ and $|\sqrt{2\mu}e^{i\theta_2}\rangle_{b_0,+45^\circ}$, at a $50:50$ BS. The output states in modes a_1 and b_1 (see Figure 1) are given by

$$|\sqrt{\mu}(e^{i\theta_1}+e^{i\theta_2})\rangle_{a_1,+45^\circ}\otimes|\sqrt{\mu}(e^{i\theta_1}-e^{i\theta_2})\rangle_{b_1,+45^\circ}. \tag{1}$$

Then, we have that the output states in modes c_1 and d_1 have the form

$$|\sqrt{\tfrac{\mu}{2}}(e^{i\theta_1}+e^{i\theta_2})\rangle_{c_1,+45^\circ}\otimes|\sqrt{\tfrac{\mu}{2}}(e^{i\theta_1}+e^{i\theta_2})\rangle_{d_1,+45^\circ}. \tag{2}$$

If these two states are combined with two coherent states of frequency w_2, $|\sqrt{\mu}e^{i\theta_3}\rangle_{a_2,+45^\circ}$ and $|\sqrt{\mu}e^{i\theta_4}\rangle_{b_2,+45^\circ}$, in a nonlinear medium using the SFG process, the resulting output states at frequency $w_3 = w_1 + w_2$, after the polarization rotation R, can be written as (see Appendix A)

$$|\tfrac{-\sqrt{\mu}e^{i\theta_3}(e^{i\theta_1}+e^{i\theta_2})}{\sqrt{2}}\rangle_{c_2,+45^\circ} \otimes |\tfrac{-\sqrt{\mu}e^{i\theta_4}(e^{i\theta_1}+e^{i\theta_2})}{\sqrt{2}}\rangle_{d_2,-45^\circ}. \tag{3}$$

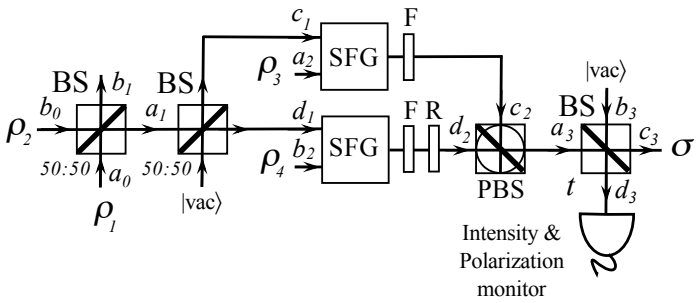

Figure 1. Basic setup of a passive decoy-state BB84 QKD source with polarization encoding using phase-randomized strong coherent pulses. The mean photon number of the signal states ρ_i, with $i \in \{1,\ldots,4\}$, can be chosen very high; for instance, $\approx 10^8$ photons. BS denotes a beamsplitter, PBS represents a polarizing beamsplitter in the $\pm 45^\circ$ linear polarization basis, such PBS transmits -45° linear polarization and reflects $+45^\circ$ linear polarization [54]. These two orthogonal linear polarizations have creation operators $a^\dagger_{\pm 45^\circ} = 1/\sqrt{2}(a^\dagger_H \pm a^\dagger_V)$. F is an optical filter, R denotes a polarization rotator changing $+45^\circ$ linear polarization to -45° linear polarization, $|\mathrm{vac}\rangle$ represents the vacuum state, and t denotes the transmittance of a BS; it satisfies $t \ll 1$.

These two beams are now re-combined at a PBS in the $\pm 45^\circ$ linear polarization basis [54]. We obtain that the output state in mode a_3 (see Figure 1) is a coherent state of the form

$$|\sqrt{\zeta(\theta)}e^{i\phi}\rangle_{\psi,a_3} = e^{-\zeta(\theta)/2}\sum_{n=0}^{\infty}\frac{\left(\sqrt{\zeta(\theta)}e^{i\phi}\right)^n}{\sqrt{n!}}|n_\psi\rangle, \tag{4}$$

where $\zeta(\theta) = 2\mu(1+\cos\theta)$, $\theta = \theta_2 - \theta_1$, $\phi = \pi + \theta_1 + \theta_3 + \arg(1+e^{i\theta})$, and the Fock states $|n_\psi\rangle$ are given by

$$|n_\psi\rangle = \frac{[\frac{1}{\sqrt{2}}(a^\dagger_{+45^\circ} + e^{i\psi}a^\dagger_{-45^\circ})]^n}{\sqrt{n!}}|\mathrm{vac}\rangle, \tag{5}$$

with $|\mathrm{vac}\rangle$ denoting the vacuum state and $\psi = \theta_4 - \theta_3$. Finally, Alice sends the quantum state given by Equation (4) through a BS of transmittance $t \ll 1$. Then, the output states in modes c_3 and d_3 are given by

$$|\sqrt{t\zeta(\theta)}e^{i\phi}\rangle_{\psi,c_3} \otimes |\sqrt{(1-t)\zeta(\theta)}e^{i\phi}\rangle_{\psi,d_3}. \tag{6}$$

The analysis of the case where the global phase of each input signal ρ_i, with $i \in \{1,\ldots,4\}$, is randomized and inaccessible to the eavesdropper is now straightforward. It can be solved by just

integrating the signals $|\sqrt{t\zeta(\theta)}e^{i\phi}\rangle_{\psi,c_3}$ and $|\sqrt{(1-t)\zeta(\theta)}e^{i\phi}\rangle_{\psi,d_3}$ given by Equation (6) over all angles θ, ϕ, and ψ. In particular, we have that the output state σ in this scenario (see Figure 1) can be written as

$$\begin{aligned}\sigma &= \frac{1}{(2\pi)^3}\iiint_{\phi,\theta,\psi} |\sqrt{t\zeta(\theta)}e^{i\phi}\rangle_{\psi,c_3}\langle\sqrt{t\zeta(\theta)}e^{i\phi}|\,\mathrm{d}\phi\mathrm{d}\theta\mathrm{d}\psi \\ &= \frac{1}{(2\pi)^2}\int_{\theta} e^{-\gamma(\theta)}\sum_{n=0}^{\infty}\frac{\gamma(\theta)^n}{n!}\int_{\psi}|n_\psi\rangle\langle n_\psi|\,\mathrm{d}\theta\mathrm{d}\psi, \end{aligned} \tag{7}$$

where the intensity $\gamma(\theta)$ is given by $\gamma(\theta) = t\zeta(\theta)$. As already mentioned previously, note that the generation of phase-randomized coherent states can be achieved, for example, by using strong current modulation of the laser diode, well above and below threshold, which ensures a true random phase (unknown to the eavesdropper) for each prepared pulse [21,22].

The weak intensity signal σ in mode c_3 is suitable for QKD and Alice sends it to Bob through the quantum channel. In addition, she uses the strong intensity signal available in mode d_3 to measure both its intensity and polarization. This last measurement can be realized, for example, by means of a passive BB84 detection scheme where the basis choice is performed by a $50:50$ BS, and on each end there is a PBS and two classical photodetectors. From the different intensities observed in each of these four photodetectors, Alice can determine both the value of the angle ψ and the total intensity of the signal. Note that, by assumption, we have that the intensity of the input states ρ_i is very high.

Intuitively speaking, the working principle of the setup illustrated in Figure 1 is quite simple. In a first step, the setup passively generates in mode a_1 coherent states of random amplitude. This is done by combining two coherent states or equal amplitude but random phase at a BS. This part follows the approach proposed in [37,38] to passively prepare decoy states. Then, in a second step, the setup generates signals whose photons are randomly polarized within the X-Z plane of the Bloch sphere. For this, it first prepares two phase-randomized coherent states of the same amplitude in $+45^\circ$ and -45° linear polarization, and then interferes them at a PBS. This approach is inspired by the solution introduced in [42]. Indeed, this is the role of the interferometric part of the scheme, where the SFG process is actually used to imprint a random phase to each state. Finally, in a third step, the setup attenuates the generated signals to the single-photon level before they are sent to Bob, and it also determines both the intensity and polarization of the signals prepared.

For simplicity, let us assume for the moment that the polarization measurement is perfect, *i.e.*, for each incoming signal it provides Alice with a precise value for the measured angle ψ, while the intensity measurement only tells her whether the measured intensity is below or above a certain threshold value Λ that satisfies $0 < \Lambda < 4\mu(1-t)$. That is, Λ is between the minimal and maximal possible values of the intensity $(1-t)\zeta(\theta)$ of the optical pulses in mode d_3. The first intensity interval, $\xi_d = [0, \Lambda]$, can be associated, for instance, to the generation of a decoy state in output mode c_3 (that we shall denote as σ_d), while the second intensity interval, $\xi_s = [\Lambda, 4\mu(1-t)]$, corresponds to the case of preparing a signal state (σ_s). Note, however, that the analysis presented in this section can be straightforwardly adapted to cover as well the case of several intensity intervals ξ_i (*i.e.*, the generation of several decoy states). Figure 2 (case A) shows a graphical representation of the intensity $(1-t)\zeta(\theta)$ in mode d_3 versus the angle θ, together with the threshold value Λ and the intensity intervals ξ_d and ξ_s.

The threshold angle θ_Λ that satisfies $(1-t)\zeta(\theta_\Lambda) = \Lambda$ is given by

$$\theta_\Lambda = \arccos\left(\frac{\Lambda}{2\mu(1-t)} - 1\right). \tag{8}$$

In this simplified scenario, the conditional quantum states that are sent to Bob can be written as

$$\sigma_{i,\psi} = \sum_{n=0}^{\infty} p_n^i |n_\psi\rangle\langle n_\psi|, \tag{9}$$

where $i = \{s, d\}$, and the probabilities p_n^i are given by

$$\begin{aligned} p_n^s &= \frac{1}{\theta_\Lambda}\int_0^{\theta_\Lambda} e^{-\gamma(\theta)}\frac{\gamma(\theta)^n}{n!}\,\mathrm{d}\theta, \\ p_n^d &= \frac{1}{\pi-\theta_\Lambda}\int_{\theta_\Lambda}^{\pi} e^{-\gamma(\theta)}\frac{\gamma(\theta)^n}{n!}\,\mathrm{d}\theta. \end{aligned} \tag{10}$$

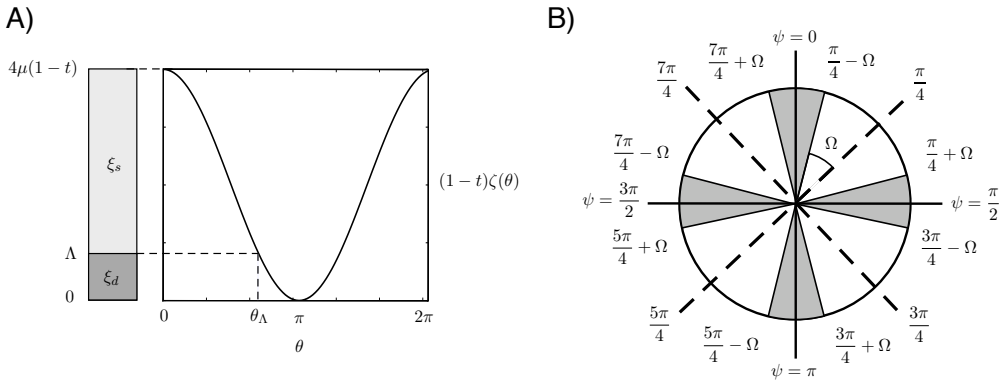

Figure 2. (Case A) Graphical representation of the intensity $(1-t)\zeta(\theta)$ in mode d_3 (see Figure 1) versus the angle θ. Λ represents the threshold value of the classical intensity measurement, θ_Λ is its associated threshold angle, and ξ_d and ξ_s denote the resulting intensity intervals. (Case B) Graphical representation of the valid regions for the angle ψ. These regions are marked in gray. They depend on an acceptance parameter $\Omega \in [0, \pi/4]$.

In practice, however, it is not necessary that Alice determines the value of ψ accurately and restricts herself to only those events where she actually prepares a perfect BB84 polarization state (*i.e.*, when the angle ψ satisfies $\psi \in \{0, \pi/2, \pi, 3\pi/2\}$) [42]. Note that the probability associated with these ideal events tends to zero. Instead, it is sufficient if the polarization measurement tells her the value of ψ within a certain interval around the desired ideal values. This situation is illustrated in Figure 2 (case B), where Alice selects some valid regions (marked with gray color in the figure) for the angle ψ [42]. These regions depend on an acceptance parameter $\Omega \in [0, \pi/4]$ that we optimize. In particular, whenever the value of ψ lies within any of the valid regions, Alice considers the pulse emitted by the source as a valid signal. Otherwise, the pulse is discarded afterwards during the post-processing phase of the protocol, and it does not contribute to the key rate. The probability that a pulse is accepted, p_{acc}, is given by

$$p_{\mathrm{acc}} = 1 - \frac{4\Omega}{\pi}. \tag{11}$$

There is a trade-off on the acceptance parameter Ω. A high acceptance probability p_{acc} favors $\Omega \approx 0$, but this action also results in an increase of the quantum bit error rate (QBER) of the protocol. A low QBER favors $\Omega \approx \pi/4$, but then $p_{\text{acc}} \approx 0$. Note that in the limit where Ω tends to $\pi/4$ we recover the standard decoy-state BB84 protocol.

3. Lower Bound on the Secret Key Rate

We shall consider that Alice and Bob treat decoy and signal states separately, and they distill secret key from both of them. For that, we use the security analysis presented in [6], which combines the results provided by Gottesman–Lo–Lütkenhaus–Preskill (GLLP) in [55] (see also [56]) with the decoy-state method. It can be shown that the single-photon signals emitted by the passive source illustrated in Figure 1, averaged over the values of Alice's key bit, are basis-independent [42]. This analysis is valid for the asymptotic regime of infinitely long keys. The secret key rate formula can be written as

$$R \geq \sum_i p_i \max\{R^i, 0\}, \tag{12}$$

with $i = \{s, d\}$. Here p_i denotes the probability to generate a state associated to the intensity interval ξ_i (*i.e.*, $p_s = \theta_\Lambda/\pi$ and $p_d = 1 - p_s$), and

$$R^i \geq q p_{\text{acc}} \big\{ -Q^i f(E^i) H(E^i) + p_1^i Y_1 [1 - H(e_1)] + p_0^i Y_0 \big\}. \tag{13}$$

The parameter q is the efficiency of the protocol ($q = 1/2$ for the standard BB84 scheme, and $q \approx 1$ for its efficient version [57]); Q^i denotes the gain, *i.e.*, the probability that Bob obtains a click in his measurement apparatus when Alice sends him a signal σ_i; $f(E^i)$ represents the efficiency of the error correction protocol as a function of the error rate E^i, typically $f(E^i) \geq 1$ with Shannon limit $f(E^i) = 1$ [58]; Y_n is the yield of an n-photon signal, *i.e.*, the conditional probability of a detection event on Bob's side given that Alice transmits an n-photon state; e_n denotes the error rate of an n-photon signal; and $H(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$ represents the binary Shannon entropy function.

For simulation purposes, we shall consider a simple channel model in the absence of eavesdropping [6,59]; it consists of a BS whose transmittance depends on the transmission distance and on the loss coefficient of the quantum channel. That is, for simplicity, we neglect any misalignment effect in the channel. Furthermore, we assume that Bob employs an active BB84 detection setup. This model allows us to calculate the observed experimental parameters Q^i and E^i. These quantities are given in Appendix B. Our results, however, can also be straightforwardly applied to any other channel model or detection setup, as they depend only on the observed gain and QBER.

To evaluate the secret key rate formula given by Equation (13) we need to estimate the yields Y_0 and Y_1, together with the single-photon error rate e_1, by solving the following set of linear equations:

$$Q^i = \sum_{n=0}^{\infty} p_n^i Y_n, \quad \text{and} \quad Q^i E^i = \sum_{n=0}^{\infty} p_n^i Y_n e_n. \tag{14}$$

For that, we shall use the procedure proposed in [38,59]. Moreover, we will assume a random background (*i.e.*, $e_0 = 1/2$).

This method requires that the probabilities p_n^i given by Equation (10) satisfy certain conditions that we confirm numerically. The results are included in Appendix C. It is important to emphasize, however, that the estimation technique presented in [38,59] only constitutes a possible example of a finite decoy-state setting estimation procedure. In principle, many other estimation methods are also available for this purpose, such as linear programming tools [60], which might result in sharper, or for the purpose of QKD, better bounds on the considered probabilities.

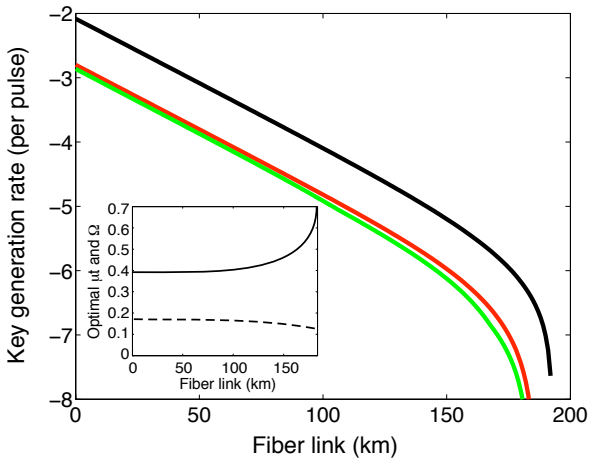

Figure 3. Lower bound on the secret key rate R given by Equation (12) in logarithmic scale for the passive transmitter with two intensity settings illustrated in Figure 1 (green line). For simulation purposes, we consider the following experimental parameters: the dark count rate of Bob's detectors is $\epsilon_{\mathrm{B}} = 3.2 \times 10^{-7}$, the overall transmittance of Bob's detection apparatus is $\eta_{\mathrm{B}} = 0.045$, the loss coefficient of the channel is $\alpha = 0.2$ dB/km, $q = 1/2$, and the efficiency of the error correction protocol is $f(E^i) = 1.22$. We further assume the channel model described in [6,59], where we neglect any misalignment effect. Otherwise, the actual secure distance will be smaller. The inset figure shows the value for the optimized parameters μt (dashed line) and Ω (solid line) in the passive setup. The optimal value for the threshold parameter Λ turns out to be constant with the distance and equal to $2\mu(1-t)$, *i.e.*, the threshold angle θ_Λ satisfies $\theta_\Lambda = \pi/2$. The black line represents a lower bound on R for an active asymptotic decoy-state BB84 system with infinite decoy settings [6], while the red line shows the case of a passive transmitter with infinite intensity intervals ξ_i (see Appendix D).

The resulting lower bound on the secret key rate with two intensity settings is illustrated in Figure 3 (green line). In our simulation we employ the following experimental parameters: the dark count rate of Bob's detectors is $\epsilon_{\mathrm{B}} = 3.2 \times 10^{-7}$, the overall transmittance of Bob's detection apparatus is $\eta_{\mathrm{B}} = 0.045$, and the loss coefficient of the channel is $\alpha = 0.2$ dB/km. We further assume that $q = 1/2$, and $f(E^i) = 1.22$. With this configuration, it turns out that the optimal value of the parameter μt decreases with increasing distance, while the optimal value of the parameter Ω increases with the distance. A similar behavior was also observed in the passive BB84 transmitter (without decoy states) proposed in [42]. In particular, μt diminishes from ≈ 0.175 to ≈ 0.125, while Ω augments from ≈ 0.393 to ≈ 0.7. At long distances the gain of the protocol is very low and, therefore, it is important to keep both the

multi-photon probability of the source (related with the parameter μt) and the intrinsic error rate of the signals sent by Alice (related with the parameter Ω) also low. Figure 3 includes as well an inset plot with the optimized parameters μt (dashed line) and Ω (solid line). The optimal value for the parameter Λ turns out to be constant with the distance; it is given by $\Lambda = 2\mu(1-t)$, *i.e.*, the threshold angle θ_Λ is equal to $\pi/2$. This figure also shows a lower bound on the secret key rate for the cases of an active decoy-state BB84 system with infinite decoy settings (black line) [6], and a passive transmitter with infinite intensity intervals ξ_i (red line). The cutoff points where the secret key rate drops down to zero are ≈ 181 km (passive setup with two intensity settings), ≈ 183 km (passive setup with infinite intensity settings), and ≈ 192 km (active transmitter with infinite decoy settings). From the results shown in Figure 3 we see that the performance of the passive transmitter presented in Section 2, with only two intensity settings, is similar to that of an active asymptotic setup, thus showing the practical interest of the passive scheme. The relatively small difference between the achievable secret key rates in both scenarios is due to two main factors: (a) the intrinsic error rate of the signals accepted by Alice, which is zero only in the case of an active source; and (b) the probability p_{acc} to accept a pulse emitted by the source, which is $p_{acc} < 1$ in the passive setup and $p_{acc} = 1$ in the active scheme. For instance, we have that for most distances $\Omega \approx 0.393$, which implies $p_{acc} \approx 0.5$. This fact reduces the key rate on logarithmic scale of the passive transmitter by a factor of $\log_{10} p_{acc} \approx 0.3$. The additional factor of ≈ 0.45 that can be observed in Figure 3 arises mainly from the intrinsic error rate of the signals.

4. Phase Encoding

Similar ideas to the ones presented in Section 2 can also be used in other implementations of the decoy-state BB84 protocol with a different signal encoding. For instance, in those QKD experiments based on phase encoding, which is more suitable to use with optical fibers than polarization encoding, which is particularly relevant in the context of free-space QKD [1,2].

The basic setup is illustrated in Figure 4.

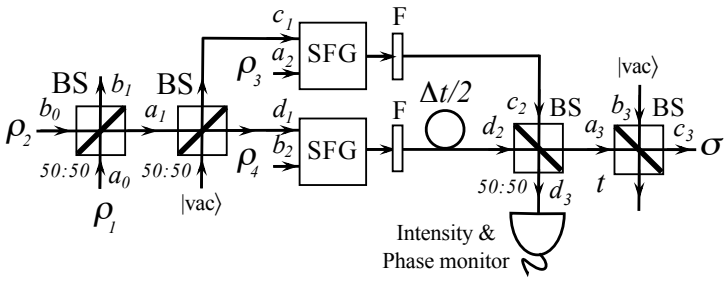

Figure 4. Basic setup of a passive decoy-state BB84 QKD source with phase encoding. The delay introduced by one arm of the interferometer is equal to half the time difference Δt between two consecutive pulses.

Again, for simplicity, let us consider first the case where the input signals ρ_i, with $i \in \{1,\ldots,4\}$, are pure coherent states with arbitrary phase relationship: $|\sqrt{2\mu}e^{i\theta_1}\rangle_{a_0,+45^\circ}$ and $|\sqrt{2\mu}e^{i\theta_2}\rangle_{b_0,+45^\circ}$ (of frequency w_1), and $|\sqrt{\mu}e^{i\theta_3}\rangle_{a_2,+45^\circ}$ and $|\sqrt{\mu}e^{i\theta_4}\rangle_{b_2,+45^\circ}$ (of frequency w_2). Let Δt denote the time

difference between two consecutive pulses generated by the sources. Then, from Section 2 we have that the signals in modes c_2 and d_2 at time instances t and $t + \Delta t/2$ can be written as

$$|\sqrt{\tfrac{\zeta(\theta)}{2}}e^{i\phi}\rangle^{t}_{c_2,+45^\circ} \otimes |\sqrt{\tfrac{\zeta(\theta)}{2}}e^{i\phi'}\rangle^{t+\Delta t/2}_{d_2,+45^\circ}, \tag{15}$$

where $\phi' = \phi + \theta_4 - \theta_3$. Similarly, we find that the quantum states in modes c_3 and d_3 are given by, respectively,

$$\begin{aligned} |\tfrac{\sqrt{\gamma(\theta)}}{2}e^{i\phi}\rangle^{t}_{c_3,+45^\circ} \quad &\otimes \quad |\tfrac{\sqrt{\gamma(\theta)}}{2}e^{i\phi'}\rangle^{t+\Delta t/2}_{c_3,+45^\circ}, \\ |\tfrac{\sqrt{\zeta(\theta)}}{2}e^{i\phi}\rangle^{t}_{d_3,+45^\circ} \quad &\otimes \quad |\tfrac{\sqrt{\zeta(\theta)}}{2}e^{i\phi'}\rangle^{t+\Delta t/2}_{d_3,+45^\circ}. \end{aligned} \tag{16}$$

The case of phase-randomized strong coherent pulses is completely analogous to that of Section 2 and we omit it here for simplicity; it results in an uniform distribution for the angles θ, ϕ, and ϕ' for both pairs of pulses given by Equation (16). The strong signals in mode d_3 are used to measure both their phases, relative to some local reference phase, and their intensities by means of an intensity and phase measurement, while Alice sends the weak signals in mode c_3 to Bob. Again, just like in the passive source with polarization encoding shown in Figure 1, Alice can now select some valid regions for the measured phases and also distinguish between different intensity settings. Then, we have that the analysis and results presented in Section 3 also apply straightforwardly to this scenario.

5. Conclusions

In this paper, we have introduced a complete passive transmitter for QKD that can prepare decoy-state Bennett-Brassard 1984 signal states using coherent light. Our method employs sum-frequency generation together with linear optical components and classical photodetectors. In the asymptotic limit of an infinite long experiment, we have proven that such passive scheme can provide a secret key rate (per pulse) lower but comparable to the one delivered by an active decoy-state BB84 setup with infinite decoy settings. In practice, however, it is uncertain if the passive scheme will be able to beat active transmitters or passive solutions based on PDC sources in general; the answer will depend on various technologies [63,64].

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

Acknowledgments

We thank F. Steinlechner for helpful discussions. This work was supported by the Galician Regional Government (program "Ayudas para proyectos de investigación desarrollados por investigadores emergentes", and consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO) project MAGO (Ref. FIS2011-23520), the "Fondo Europeo de Desarrollo Regional" (FEDER) through grants TEC2013-46168-R and TEC2014-54898-R, and the European Research Council project AQUMET.

Author Contributions

All authors contributed extensively to the work presented in this paper. All authors have read and approved the final manuscript.

Appendix

A. Sum-Frequency Generation

For completeness, in this Appendix we include the calculations to derive Equation (3) in Section 2. Our starting point are the input states to one of the two SFG processes used in the passive transmitter illustrated in Figure 1: $|\sqrt{\frac{\mu}{2}}(e^{i\theta_1}+e^{i\theta_2})\rangle_{c_1,+45^\circ}$ and $|\sqrt{\mu}e^{i\theta_3}\rangle_{a_2,+45^\circ}$. Such process is described by the Hamiltonian $H = i\hbar\chi(c_1 a_2 c_2^\dagger - \text{H.c.})$, where $c_2^\dagger$ represents the creation operator for the light wave at frequency $w_3 = w_1 + w_2$ [45]. The parameter χ is a coupling constant that is proportional to the second-order susceptibility $\chi^{(2)}$ of the nonlinear material, and H.c. denotes a Hermitian conjugate. When the pump mode at frequency w_2 is kept strong and undepleted, then this mode can be typically treated classically as a complex number. With this assumption, we have that the effective Hamiltonian above can now be written as $H = i\hbar\chi(\sqrt{\mu}e^{i\theta_3}c_1 c_2^\dagger - \text{H.c.})$. Using the Heisenberg equation of motion, it is straightforward to obtain the following coupled-mode equations:

$$\frac{\mathrm{d}c_1}{\mathrm{d}t} = -\chi\sqrt{\mu}e^{-i\theta_3}c_2, \quad \frac{\mathrm{d}c_2}{\mathrm{d}t} = \chi\sqrt{\mu}e^{i\theta_3}c_1, \tag{17}$$

which can be solved in terms of initial values at $t = 0$ to yield

$$\begin{aligned} c_1(t) &= c_1(0)\cos(\sqrt{\mu}\chi t) - e^{-i\theta_3}c_2(0)\sin(\sqrt{\mu}\chi t) \\ c_2(t) &= c_2(0)\cos(\sqrt{\mu}\chi t) + e^{i\theta_3}c_1(0)\sin(\sqrt{\mu}\chi t). \end{aligned} \tag{18}$$

At the point of complete conversion, $t_c = \pi/(2\sqrt{\mu}\chi)$, we obtain

$$c_1^\dagger(t_c) = -e^{i\theta_3}c_2^\dagger(0), \quad c_2^\dagger(t_c) = e^{-i\theta_3}c_1^\dagger(0). \tag{19}$$

That is, at time t_c we find that the resulting output state at frequency w_3 from the SFG process is given by

$$|-\sqrt{\tfrac{\mu}{2}}e^{i\theta_3}(e^{i\theta_1}+e^{i\theta_2})\rangle_{c_2,+45^\circ}. \tag{20}$$

B. Gain and QBER

In this Appendix, we obtain a mathematical expression for the observed gains Q^i and error rates E^i, with $i \in \{s, d\}$, for the passive QKD transmitter with two intensity settings introduced in Section 2. For that, we employ the typical channel model in the absence of eavesdropping [6,59]; it just consists of a BS of transmittance $\eta_{\text{channel}} = 10^{-\frac{\alpha d}{10}}$, where α denotes the loss coefficient of the channel measured in dB/km and d is the transmission distance. Moreover, for simplicity, we consider that Bob employs an active BB84 detection setup with two threshold detectors.

The action of Bob's measurement device can be described by two positive operator value measures (POVMs), one for each of the two BB84 polarization bases $\beta \in \{l, c\}$, with l denoting a linear

polarization basis and c a circular polarization basis. Each POVM contains four elements: G^{β}_{vac}, G^{β}_{0}, G^{β}_{1}, and G^{β}_{dc}. The first one corresponds to the case of no click in the detectors, the following two POVM operators give precisely one detection click, and the last one, G^{β}_{dc}, gives rise to both detectors being triggered. These operators can be written as [42]

$$\begin{aligned} G^{\beta}_{\mathrm{vac}} &= [1-\epsilon_{\mathrm{B}}(2-\epsilon_{\mathrm{B}})]F^{\beta}_{\mathrm{vac}}, \\ G^{\beta}_{0} &= (1-\epsilon_{\mathrm{B}})\epsilon_{\mathrm{B}}F^{\beta}_{\mathrm{vac}} + (1-\epsilon_{\mathrm{B}})F^{\beta}_{0}, \\ G^{\beta}_{1} &= (1-\epsilon_{\mathrm{B}})\epsilon_{\mathrm{B}}F^{\beta}_{\mathrm{vac}} + (1-\epsilon_{\mathrm{B}})F^{\beta}_{1}, \\ G^{\beta}_{\mathrm{dc}} &= I - G^{\beta}_{\mathrm{vac}} - G^{\beta}_{0} - G^{\beta}_{1}. \end{aligned} \tag{21}$$

Here we assume that the background rate is, to a good approximation, independent of the signal detection. Moreover, for easiness of notation, we consider only a background contribution coming from the dark count rate ϵ_{B} of Bob's detectors and we neglect other background contributions like, for instance, stray light arising from timing pulses which are not completely filtered out in reception. The operators F^{β}_{vac}, F^{β}_{0}, F^{β}_{1}, and F^{β}_{dc} have the form

$$\begin{aligned} F^{\beta}_{\mathrm{vac}} &= \sum_{n,m=0}^{\infty} (1-\eta_{\mathrm{sys}})^{n+m} |n,m\rangle_{\beta}\langle n,m|, \\ F^{\beta}_{0} &= \sum_{n,m=0}^{\infty} [1-(1-\eta_{\mathrm{sys}})^{n}](1-\eta_{\mathrm{sys}})^{m} |n,m\rangle_{\beta}\langle n,m|, \\ F^{\beta}_{1} &= \sum_{n,m=0}^{\infty} [1-(1-\eta_{\mathrm{sys}})^{m}](1-\eta_{\mathrm{sys}})^{n} |n,m\rangle_{\beta}\langle n,m|, \\ F^{\beta}_{\mathrm{dc}} &= \sum_{n,m=0}^{\infty} [1-(1-\eta_{\mathrm{sys}})^{n}][1-(1-\eta_{\mathrm{sys}})^{m}] \times |n,m\rangle_{\beta}\langle n,m|, \end{aligned} \tag{22}$$

with $\beta \in \{l,c\}$. The signals $|n,m\rangle_{l}$ ($|n,m\rangle_{c}$) represent the state which has n photons in the horizontal (circular left) polarization mode and m photons in the vertical (circular right) polarization mode. The parameter η_{sys} denotes the overall transmittance of the system. This quantity can be written as $\eta_{\mathrm{sys}} = \eta_{\mathrm{B}}\eta_{\mathrm{channel}}$, where η_{B} is the overall transmittance of Bob's detection apparatus, *i.e.*, it includes the transmittance of any optical component within Bob's measurement device together with the efficiency of his detectors.

In the scenario considered, it turns out that the gains Q^{i} are independent of the actual polarization of the signals $\sigma_{i,\psi}$ given by Equation (9) and the basis β used to measure them. We obtain

$$Q^{i} = 1 - \mathrm{Tr}\big(G^{\beta}_{\mathrm{vac}}\sigma_{i,\psi}\big) = 1 - \frac{(1-\epsilon_{\mathrm{B}})^{2}}{p_{i}\pi}\int_{\theta_{\xi_{i}}} e^{-\eta_{\mathrm{sys}}\gamma(\theta)}\,\mathrm{d}\theta, \tag{23}$$

where $p_{s} = \theta_{\Lambda}/\pi$, $p_{d} = 1-p_{s}$, $\theta_{\xi_{s}} = [0,\theta_{\Lambda}]$, and $\theta_{\xi_{d}} = [\theta_{\Lambda},\pi]$.

When $\theta_{\Lambda} = \pi/2$, which is the value that maximizes the secret key rate formula given by Equation (12), we have that the gains Q^{i} can be written as

$$\begin{aligned} Q^{s} &= 1-(1-\epsilon_{\mathrm{B}})^{2}A_{-}(\eta_{\mathrm{sys}}\zeta), \\ Q^{d} &= 1-(1-\epsilon_{\mathrm{B}})^{2}A_{+}(\eta_{\mathrm{sys}}\zeta), \end{aligned} \tag{24}$$

where $\zeta = 2\mu t$, and

$$A_{\pm}(x) = e^{-x}\big[I_{0,x} \pm L_{0,x}\big]. \tag{25}$$

Here $I_{q,z}$ represents the modified Bessel function of the first kind, and $L_{q,z}$ denotes the modified Struve function. These functions are defined as [61,62]

$$\begin{aligned} I_{q,z} &= \frac{1}{2\pi i}\oint e^{(z/2)(t+1/t)}t^{-q-1}dt, \\ L_{q,z} &= \frac{z^q}{2^{q-1}\sqrt{\pi}\Gamma_{q+1/2}}\int_0^{\pi/2}\sinh\left(z\cos\theta\right)\sin\theta^{2q}d\theta. \end{aligned} \tag{26}$$

The error rates E^i depend on the value of the angle ψ. By symmetry, we can restrict ourselves to evaluate the QBER in only one of the valid regions for ψ. Note that is the same in all of them. For instance, let us consider the case where $\psi \in [7\pi/4 + \Omega, \pi/4 - \Omega]$ (which corresponds to the horizontal polarization interval), and let E^i_{ψ} denote the error rate of a signal $\sigma_{i,\psi}$ in that region. This quantity can be written as

$$E^i_{\psi} = \frac{1}{Q^i}\mathrm{Tr}\left[\left(G^l_1 + \frac{1}{2}G^l_{\mathrm{dc}}\right)\sigma_{i,\psi}\right]. \tag{27}$$

Here we have considered the typical initial post-processing step in the BB84 protocol, where double-click events are not discarded by Bob, but are randomly assigned to single-click events. Equation (27) can be further simplified as

$$E^i_{\psi} = \frac{1}{2Q^i}\big\{\epsilon_{\mathrm{B}}(\epsilon_{\mathrm{B}}-1)f^i_{0,\psi} + [2+\epsilon_{\mathrm{B}}(\epsilon_{\mathrm{B}}-3)]f^i_{1,\psi} + (1-\epsilon_{\mathrm{B}})^2 f^i_{\mathrm{dc},\psi} + \epsilon_{\mathrm{B}}(2-\epsilon_{\mathrm{B}})\big\}, \tag{28}$$

where $f^i_{j,\psi} = \mathrm{Tr}\big(F^l_j\sigma^i_{i,\psi}\big)$. After a short calculation, we obtain

$$\begin{aligned} f^i_{0,\psi} &= \frac{1}{p_i\pi}\int_{\theta_{\xi_i}} e^{-\eta_{\mathrm{sys}}\gamma(\theta)}\Big[-1+e^{\frac{1}{2}\eta_{\mathrm{sys}}\gamma(\theta)(1+\cos\psi)}\Big]\,\mathrm{d}\theta, \\ f^i_{1,\psi} &= \frac{1}{p_i\pi}\int_{\theta_{\xi_i}} e^{-\eta_{\mathrm{sys}}\gamma(\theta)}\Big[-1+e^{\frac{1}{2}\eta_{\mathrm{sys}}\gamma(\theta)(1-\cos\psi)}\Big]\,\mathrm{d}\theta, \\ f^i_{\mathrm{dc},\psi} &= 1+\frac{1}{p_i\pi}\int_{\theta_{\xi_i}} e^{-\eta_{\mathrm{sys}}\gamma(\theta)} - e^{-\frac{1}{2}\eta_{\mathrm{sys}}\gamma(\theta)(1-\cos\psi)} - e^{-\frac{1}{2}\eta_{\mathrm{sys}}\gamma(\theta)(1+\cos\psi)}\,\mathrm{d}\theta. \end{aligned} \tag{29}$$

when $\theta_{\Lambda} = \pi/2$, these expressions can be simplified as

$$\begin{aligned} f^s_{0,\psi} &= -A_-(\eta_{\mathrm{sys}}\zeta) + A_-[\kappa_+(\psi)], \\ f^d_{0,\psi} &= -A_+(\eta_{\mathrm{sys}}\zeta) + A_+[\kappa_+(\psi)], \\ f^s_{1,\psi} &= -A_-(\eta_{\mathrm{sys}}\zeta) + A_-[\kappa_-(\psi)], \\ f^d_{1,\psi} &= -A_+(\eta_{\mathrm{sys}}\zeta) + A_+[\kappa_-(\psi)], \\ f^s_{\mathrm{dc},\psi} &= 1 + A_-(\eta_{\mathrm{sys}}\zeta) - A_-[\epsilon_+(\psi)] - A_-[\epsilon_-(\psi)], \\ f^d_{\mathrm{dc},\psi} &= 1 + A_+(\eta_{\mathrm{sys}}\zeta) - A_+[\epsilon_+(\psi)] - A_+[\epsilon_-(\psi)], \end{aligned} \tag{30}$$

where the parameters $\kappa_{\pm}(\psi)$ and $\epsilon_{\pm}(\psi)$ have the form

$$\begin{aligned} \kappa_{\pm}(\psi) &= \eta_{\mathrm{sys}}\zeta[1-(1\pm\cos\psi)/2], \\ \epsilon_{\pm}(\psi) &= \eta_{\mathrm{sys}}\zeta(1\pm\cos\psi)/2. \end{aligned} \tag{31}$$

The quantum bit error rates E^i are then given by

$$E^i = \frac{2}{\pi - 4\Omega} \int_{\frac{7\pi}{4}+\Omega}^{\frac{\pi}{4}-\Omega} E^i_\psi \mathrm{d}\psi. \tag{32}$$

Combining Equations (28) and (30)–(32), we find that

$$\begin{aligned} E^s \;=\; & \frac{1}{2Q^s}\Bigg\{1 - (1-\epsilon_{\mathrm{B}})^2 A_-(\eta_{\mathrm{sys}}\zeta) + \frac{2}{\pi - 4\Omega}\int_{\frac{7\pi}{4}+\Omega}^{\frac{\pi}{4}-\Omega} \epsilon_{\mathrm{B}}(\epsilon_{\mathrm{B}}-1) A_-[\kappa_+(\psi)] \\ & + [2 + \epsilon_{\mathrm{B}}(\epsilon_{\mathrm{B}}-3)] A_-[\kappa_-(\psi)] - (1-\epsilon_{\mathrm{B}})^2 \big[A_-[\epsilon_+(\psi)] + A_-[\epsilon_-(\psi)]\big]\mathrm{d}\psi\Bigg\}, \end{aligned} \tag{33}$$

and

$$\begin{aligned} E^d \;=\; & \frac{1}{2Q^d}\Bigg\{1 - (1-\epsilon_{\mathrm{B}})^2 A_+(\eta_{\mathrm{sys}}\zeta) + \frac{2}{\pi - 4\Omega}\int_{\frac{7\pi}{4}+\Omega}^{\frac{\pi}{4}-\Omega} \epsilon_{\mathrm{B}}(\epsilon_{\mathrm{B}}-1) A_+[\kappa_+(\psi)] \\ & + [2 + \epsilon_{\mathrm{B}}(\epsilon_{\mathrm{B}}-3)] A_+[\kappa_-(\psi)] - (1-\epsilon_{\mathrm{B}})^2 \big[A_+[\epsilon_+(\psi)] + A_+[\epsilon_-(\psi)]\big]\mathrm{d}\psi\Bigg\}, \end{aligned} \tag{34}$$

and we solve these equations numerically.

C. Estimation procedure

The secret key rate formula given by Equation (13) can be lower bounded by

$$R^i \geq q p_{\mathrm{acc}} \big\{ - Q^i f(E^i) H(E^i) + (p^i_1 Y_1 + p^i_0 Y_0)[1 - H(e^U_1)]\big\}, \tag{35}$$

where e^U_1 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 $p^i_1 Y_1 + p^i_0 Y_0$ for all $i \in \{s, d\}$, together with e^U_1. For that, we can directly use the results obtained in [38], which we include in this Appendix for completeness. The probabilities p^i_n given by Equation (10) need to satisfy certain conditions that we confirm numerically. In particular, we have that

$$p^i_1 Y_1 + p^i_0 Y_0 \geq \max\left\{ \frac{p^i_1 (p^d_2 Q^s - p^s_2 Q^d)}{p^d_2 p^s_1 - p^s_2 p^d_1} + \left[p^i_0 - p^i_1 \frac{p^d_2 p^s_0 - p^s_2 p^d_0}{p^d_2 p^s_1 - p^s_2 p^d_1}\right] Y^U_0, 0 \right\}, \tag{36}$$

where Y^U_0 denotes an upper bound on the background rate Y_0 given by

$$Y_0 \leq Y^U_0 = \min\left\{ \frac{E^d Q^d}{p^d_0 e_0}, \frac{E^s Q^s}{p^s_0 e_0}, 1 \right\}, \tag{37}$$

with $e_0 = 1/2$. The single-photon error rate e_1 can be upper bounded as

$$e_1 \leq e^U_1 = \min\left\{ \frac{E^d Q^d - p^d_0 Y^L_0 e_0}{p^d_1 Y^L_1}, \frac{E^s Q^s - p^s_0 Y^L_0 e_0}{p^s_1 Y^L_1}, \frac{p^s_0 E^d Q^d - p^d_0 E^s Q^s}{(p^d_1 p^s_0 - p^s_1 p^d_0) Y^L_1} \right\}, \tag{38}$$

where Y_1^L and Y_0^L represent, respectively, a lower bound on the yield Y_1 and the background rate Y_0. These quantities are given by

$$Y_1 \geq Y_1^L = \max\left\{\frac{p_2^d Q^s - p_2^s Q^d - (p_2^d p_0^s - p_2^s p_0^d) Y_0^U}{p_2^d p_1^s - p_2^s p_1^d}, 0\right\}, \tag{39}$$

and

$$Y_0 \geq Y_0^L = \max\left\{\frac{p_1^d Q^s - p_1^s Q^d}{p_1^d p_0^s - p_1^s p_0^d}, 0\right\}. \tag{40}$$

To evaluate these expressions we need the statistics p_n^i for $n = 0, 1, 2$. Using Equation (10), and assuming again $\theta_\Lambda = \pi/2$, we obtain

$$\begin{aligned} p_0^s &= A_-(\zeta), \\ p_1^s &= \zeta[A_-(\zeta) - e^{-\zeta}(I_{1,\zeta} - L_{-1,\zeta})], \\ p_2^s &= \frac{\zeta}{2}\left\{\zeta A_-(\zeta) + e^{-\zeta}\left[\frac{2}{\pi}\left(1 - \frac{\zeta^2}{3}\right) + (1-2\zeta)(I_{1,\zeta} - L_{-1,\zeta}) + \zeta(I_{2,\zeta} - L_{2,\zeta})\right]\right\}, \end{aligned} \tag{41}$$

and

$$\begin{aligned} p_0^d &= A_+(\zeta), \\ p_1^d &= \zeta[A_+(\zeta) - e^{-\zeta}(I_{1,\zeta} + L_{-1,\zeta})], \\ p_2^d &= \frac{\zeta}{2}\left\{\zeta A_+(\zeta) + e^{-\zeta}\left[-\frac{2}{\pi}\left(1 - \frac{\zeta^2}{3}\right) + (1-2\zeta)(I_{1,\zeta} + L_{-1,\zeta}) + \zeta(I_{2,\zeta} + L_{2,\zeta})\right]\right\}. \end{aligned} \tag{42}$$

D. Asymptotic Passive Decoy-State BB84 Transmitter

To evaluate the secret key rate formula given by Equation (12) in this scenario, we consider that $p_s \approx 1$, and we assume that Alice and Bob can estimate the relevant parameters Y_0, Y_1, and e_1 perfectly. Moreover, we use the channel and detection models introduced in Appendix B. In this situation, it turns out that the yields Y_0 and Y_1 are given by $Y_0 = \epsilon_\mathrm{B}(2 - \epsilon_\mathrm{B})$ and $Y_1 = 1 - (1 - Y_0)(1 - \eta_\mathrm{sys})$.

The single-photon error rate e_1 can be calculated using Equations (28)–(32) with $\sigma_{i,\psi} = |1_\psi\rangle\langle 1_\psi|$. After a short calculation, we obtain

$$e_1 = \frac{1}{2Y_1}\left\{Y_0 + (1-\epsilon_\mathrm{B})^2\eta_\mathrm{sys} - \frac{4(1-\epsilon_\mathrm{B})\eta_\mathrm{sys}}{\pi - 4\Omega}\sin\left(\frac{\pi}{4} - \Omega\right)\right\}. \tag{43}$$

The resulting lower bound on the secret key rate is illustrated in Figure 3 (red line) for the optimized parameters ζ and Ω.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350.

2. Lo, H.-K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2014**, *8*, 595–604.
3. Vernam, G.S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Elect. Eng.* **1926**, *45*, 109–115.
4. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984; p. 175.
5. Hwang, W.-Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **2003**, *91*, 057901.
6. Lo, H.-K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504.
7. Wang, X.-B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503.
8. Zhao, Y.; Qi, B.; Ma, X.; Lo, H.-K.; Qian, L. Experimental Quantum Key Distribution with Decoy States. *Phys. Rev. Lett.* **2006**, *96*, 070502.
9. Rosenberg, D.; Harrington, J.W.; Rice, P.R.; Hiskett, P.A.; Peterson, C.G.; Hughes, R.J.; Lita, A.E.; Nam, S.W.; Nordholt, J.E. Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber. *Phys. Rev. Lett.* **2007**, *98*, 010503.
10. Peng, C.Z.; Zhang, J.; Yang, D.; Gao, W.B.; Ma, H.X.; Yin, H.; Zeng, H.P.; Yang, T.; Wang, X.B.; Pan, J.W. Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding. *Phys. Rev. Lett.* **2007**, *98*, 010505.
11. Yuan, Z.L.; Sharpe, A.W.; Shields, A.J. Unconditionally secure one-way quantum key distribution using decoy pulses. *Appl. Phys. Lett.* **2007**, *90*, 011118.
12. Dixon, A.R.; Yuan, Z.L.; Dynes, J.F.; Sharpe, A.W.; Shields, A.J. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Opt. Express* **2008**, *16*, 18790–18979.
13. Tanaka, A.; Fujiwara, M.; Nam, S.W.; Nambu, Y.; Takahashi, S.; Maeda, W.; Yoshino, K.; Miki, S.; Baek, B.; Wang, Z.; *et al*. Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. *Opt. Express* **2008**, *16*, 11354–11360.
14. Rosenberg, D.; Peterson, C.G.; Harrington, J.W.; Rice, P.R.; Dallmann, N.; Tyagi, K.T.; McCabe, K.P.; Nam, S.; Baek, B.; Hadfield, R.H.; *et al*. Practical long-distance quantum key distribution system using decoy levels. *New J. Phys.* **2009**, *11*, 045009.
15. Dixon, A.R.; Yuan, Z.L.; Dynes, J.F.; Sharpe, A.W.; Shields, A.J. Continuous operation of high bit rate quantum key distribution. *Appl. Phys. Lett.* **2010**, *96*, 161102.
16. Liu, Y.; Chen, T.-Y.; Wang, J.; Cai, W.-Q.; Wan, X.; Chen, L.-K.; Wang, J.-H.; Liu, S.-B.; Liang, H.; Yang, L.; *et al*. Decoy-State quantum key distribution with polarized photons over 200 km. *Opt. Express* **2010**, *18*, 8587–8594.
17. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Miki, S.; Yamashita, T.; Wang, Z.; Tanaka, A.; *et al*. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409.

18. Wang, J.-Y.; Yang, B.; Liao, S.-K.; Zhang, L.; Shen, Q.; Hu, X.-F.; Wu, J.-C.; Yang, S.-J.; Jiang, H.; Tang, Y.-L.; *et al*. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nat. Photonics* **2013**, *7*, 387–393.
19. Pironio, S.; Acín, A.; Massar, S.; Boyer de la Giroday, A.; Matsukevich, D.N.; Maunz, P.; Olmschenk, S.; Hayes, D.; Luo, L.; Manning, T.A.; *et al*. Random numbers certified by Bell's theorem. *Nature* **2010**, *464*, 1021–1024.
20. Williams, C.R.S.; Salevan, J.C.; Li, X.; Roy, R.; Murphy, T.E. Fast physical random number generator using amplified spontaneous emission. *Opt. Express* **2010**, *18*, 23584–23597.
21. Jofre, M.; Curty, M.; Steinlechner, F.; Anzolin, G.; Torres, J.P.; Mitchell, M.W.; Pruneri, V. True random numbers from amplified quantum vacuum. *Opt. Express* **2011**, *19*, 20665–20672.
22. Abellán, C.; Amaya, W.; Jofre, M.; Curty, M.; Acín, A.; Capmany, J.; Pruneri, V.; Mitchell, M.W. Ultra-Fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Opt. Express* **2014**, *22*, 1645–1654.
23. Qi, B.; Chi, Y.-M.; Lo, H.-K.; Qian, L. High-Speed quantum random number generation by measuring phase noise of a single-mode laser. *Opt. Lett.* **2010**, *35*, 312–314.
24. Hughes, R.J.; Nordholt, J.E.; Derkacs, D.; Peterson, C.G. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.* **2002**, *4*, doi:10.1088/1367-2630/4/1/343.
25. Kurtsiefer, C.; Zarda, P.; Halder, M.; Weinfurter, H.; Gorman, P.M.; Tapster, P.R.; Rarity, J.G. Quantum cryptography: A step towards global key distribution. *Nature* **2002**, *419*, doi:10.1038/419450a.
26. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental Quantum Cryptography. *J. Cryptol.* **1992**, *5*, 3–28.
27. Muller, A.; Bréguet, J.; Gisin, N. Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km. *Europhys. Lett.* **1993**, *23*, 383–388.
28. Muller, A.; Zbinden, H.; Gisin, N. Underwater quantum coding. *Nature* **1995**, *378*, 449, doi:10.1038/378449a0.
29. Townsend, P.D. Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems. *IEEE Photonics Tech. Lett.* **1998**, *10*, 1048–1050.
30. Xavier, G.B.; Walenta, N.; Vilela de Faria, G.; Temporão, G.P.; Gisin, N.; Zbinden, H.; von der Weid, J.P. Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation. *New J. Phys.* **2009**, *11*, 045015.
31. Hayashi, M.; Nakayama, R. Security analysis of the decoy method with the Bennett–Brassard 1984 protocol for finite key lengths. *New J. Phys.* **2014**, *16*, 063009.
32. Lim, C.C.W.; Curty, M.; Walenta, N.; Xu, F.; Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **2014**, *89*, 022307.
33. Rarity, J.G.; Owens, P.C.M.; Tapster, P.R. Quantum Random-number Generation and Key Sharing. *J. Mod. Opt.* **1994**, *41*, 2435-2444.
34. Mauerer, W.; Silberhorn, C. Quantum key distribution with passive decoy state selection. *Phys. Rev. A* **2007**, *75*, 050305(R).

35. Adachi, Y.; Yamamoto, T.; Koashi, M.; Imoto, N. Simple and Efficient Quantum Key Distribution with Parametric Down-Conversion. *Phys. Rev. Lett.* **2007**, *99*, 180503.
36. Ma, X.; Lo, H.-K. Quantum key distribution with triggering parametric down-conversion sources. *New J. Phys.* **2008**, *10*, 073018.
37. Curty, M.; Moroder, T.; Ma, X.; Lütkenhaus, N. Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution. *Opt. Lett.* **2009**, *34*, 3238–3240.
38. Curty, M.; Ma, X.; Qi, B.; Moroder, T. Passive decoy-state quantum key distribution with practical light sources. *Phys. Rev. A* **2010**, *81*, 022310.
39. Adachi, Y.; Yamamoto, T.; Koashi, M.; Imoto, N. Boosting up quantum key distribution by learning statistics of practical single-photon sources. *New J. Phys.* **2009**, *11*, 113033.
40. Ribordy, G.; Brendel, J.; Gauthier, J.-D.; Gisin, N.; Zbinden, H. Long-Distance entanglement-based quantum key distribution. *Phys. Rev. A* **2000**, *63*, 012309.
41. Tittel, W.; Brendel, J.; Zbinden, H.; Gisin, N. Quantum Cryptography Using Entangled Photons in Energy-Time Bell States. *Phys. Rev. Lett.* **2000**, *84*, 4737–4740.
42. Curty, M.; Ma, X.; Lo, H.-K.; Lütkenhaus, N. Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals. *Phys. Rev. A* **2010**, *82*, 052325.
43. Boyd, R.W. *Nonlinear Optics*; Academic Press: Waltham, MA, USA, 2008.
44. Shen, Y.R. *The Principles of Nonlinear Optics*; Wiley-Interscience: Hoboken, NJ, USA, 1984.
45. Kumar, P. Quantum frequency conversion. *Opt. Lett.* **1990**, *15*, 1476–1478.
46. Huang, J.; Kumar, P. Observation of quantum frequency conversion. *Phys. Rev. Lett.* **1992**, *68*, 2153–2156.
47. Kim, Y.-H.; Kulik, S.P.; Shih, Y. Quantum Teleportation of a Polarization State with a Complete Bell State Measurement. *Phys. Rev. Lett.* **2001**, *86*, 1370–1373.
48. Dayan, B.; Pe'er, A.; Friesem, A.A.; Silberberg, Y. Nonlinear Interactions with an Ultrahigh Flux of Broadband Entangled Photons. *Phys. Rev. Lett.* **2005**, *94*, 043602.
49. Pe'er, A.; Dayan, B.; Friesem, A.A.; Silberberg, Y. Temporal Shaping of Entangled Photons. *Phys. Rev. Lett.* **2005**, *94*, 073601.
50. Zäh, F.; Halder, M.; Feurer, T. Amplitude and phase modulation of time-energy entangled two-photon states. *Opt. Express* **2008**, *16*, 16452–16458.
51. Tanzilli, S.; Tittel, W.; Halder, M.; Alibart, O.; Baldi, P.; Gisin, N.; Zbinden, H. A photonic quantum information interface. *Nature* **2005**, *437*, 116–120.
52. Thew, R.T.; Zbinden, H.; Gisin, N. Tunable upconversion photon detector. *Appl. Phys. Lett.* **2008**, *93*, 071104.
53. Sangouard, N.; Sanguinetti, B.; Curtz, N.; Gisin, N.; Thew, R.; Zbinden, H. Faithful Entanglement Swapping Based on Sum-Frequency Generation. *Phys. Rev. Lett.* **2011**, *106*, 120403.
54. Kok, P.; Munro, W.J.; Nemoto, K.; Ralph, T.C.; Dowling, J.P.; Milburn, G.J. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.* **2007**, *79*, 135–174.
55. Gottesman, D.; Lo, H.-K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **2004**, *4*, 325–360.
56. Lo, H.-K. Getting something out of nothing. *Quantum Inf. Comput.* **2005**, *5*, 413–418.

57. Lo, H.-K.; Chau, H.F.; Ardehali, M. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. *J. Cryptol.* **2005**, *18*, 133–165.
58. Brassard, G.; Salvail, L. Secret-Key Reconciliation by Public Discussion. In *Advances in Cryptology EUROCRYPT'93*; Helleseth, T., Ed.; Springer: Berlin, Germany, 1994; pp. 410–423.
59. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326.
60. Bazaraa, M.S.; Jarvis, J.J.; Sherali, H.D. *Linear Programming and Network Flows*, 3rd ed.; Wiley: New York, NY, USA, 2004.
61. Arfken, G. *Mathematical Methods for Physicists*, 3rd ed.; Academic Press: New York, NY, USA, 1985.
62. Abramowitz, M.; Stegun, I.A. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed.; Dover: New York, NY, USA, 1972.
63. Corcoran, B.; Monat, C.; Grillet, C.; Moss, D.J.; Eggleton, B.J.; White, T.P.; O'Faolain, L.; Krauss, T.F. Green light emission in silicon through slow-light enhanced third-harmonic generation in photonic-crystal waveguides. *Nat. Photonics* **2009**, *3*, 206–210.
64. Rivoire, K.; Lin, Z.; Hatami, F.; Vučković, J. Sum-frequency generation in doubly resonant GaP photonic crystal nanocavities. *Appl. Phys. Lett.* **2010**, *97*, 043103.