Security of the Decoy-State BB84 Protocol with Imperfect State Preparation

Aleksei Reutov, Andrey Tayduganov *, Vladimir Mayboroda and Oleg Fat'yanov

Laboratory of Quantum Information Technologies, National University of Science and Technology MISIS, Moscow 119049, Russia
* Correspondence: a.taiduganov@misis.ru

Abstract: The quantum key distribution (QKD) allows two remote users to share a common information-theoretic secure secret key. In order to guarantee the security of a practical QKD implementation, the physical system has to be fully characterized and all deviations from the ideal protocol due to various imperfections of realistic devices have to be taken into account in the security proof. In this work, we study the security of the efficient decoy-state BB84 QKD protocol in the presence of the source flaws, caused by imperfect intensity and polarization modulation. We investigate the non-Poissonian photon-number statistics due to coherent-state intensity fluctuations and the basis-dependence of the source due to non-ideal polarization state preparation. The analysis is supported by the experimental characterization of intensity and phase distributions.

Keywords: quantum communication; quantum key distribution; BB84; source flaw

1. Introduction

The BB84 protocol [1] of quantum key distribution (QKD) between two distant parties, Alice and Bob, is based on the preparation and measurement of qubits in two bases (e.g., the computational Z-basis and the Hadamard X-basis), rotated relative to each other on the Bloch sphere by an angle of $\pi/2$. Any practical realization of the protocol inevitably introduces misalignments in the quantum state preparation and in the alignment of the measurement bases compared to the ideal ones, thus opening loopholes for information leakage to a potential eavesdropper (Eve). In particular, the preparation misalignments lead to the basis-dependence of the source that can allow Eve to distinguish the bases and attack two basis states separately. In the earliest security proof by Mayers [2], the source is assumed to be perfect. The simplified proof by Koashi and Preskill [3] allows the source to be uncharacterized but basis-independent. The proofs by Lo and Chau [4], Shor and Preskill [5] and Koashi [6] are all based on the *phase error* correction and assume the basis choice to be unknown to Eve. The phase error is a hypothetical error in the equivalent virtual entanglement-based protocol if the qubits of the EPR pair were measured on a complementary basis. It is well known that for an ideal source, the phase and bit error rates in two bases are equal in the asymptotic limit; that is, $E_Z^{\text{phase}} = E_X^{\text{bit}}$. However, if the source is basis-dependent, one cannot simply use one basis information to estimate the other. Thus, in this approach, the correct phase error rate estimation, taking into account the finite-key-size effects, is crucial for security analysis of the protocol with state preparation misalignments.

Further analysis by Gottesman et al. (referred to as GLLP) [7] proves the BB84 security for practical implementation of the QKD protocol when Alice's and Bob's devices are flawed. However, the GLLP approach is too conservative, it assumes the worst-case scenario when Eve can enhance the state preparation flaws by exploiting the channel loss. For this reason, the so-called *loss-tolerant* QKD protocol was proposed by Tamaki et al. [8], demonstrated experimentally [9,10] and later on developed in Refs. [11–17]. This three-state BB84-like protocol is based on the complementarity approach [6] and uses the bases

mismatch events information. Considering the imperfect phase/polarization modulation, it is demonstrated that the key rate is dramatically improved, although the phase error rate estimation technique is quite complicated.

The original BB84 protocol was described using the qubits encoded into the polarization states of a single photon. In practice, the single-photon source is approximated by weak coherent pulses generated by a highly attenuated laser. There is a non-zero probability for such a coherent state to contain multiple photons that can be exploited by Eve performing the photon-number-splitting (PNS) attack [18,19]. The invention and further development of the decoy-state method [20–23] solves this problem by introducing extra states of different intensity (mean photon number per pulse) and significantly improves the GLLP bound on the maximum secure transmission distance. For a complete formal security proof of the decoy-state method see, e.g., Ref. [24]. Due to inaccuracies of realistic intensity modulation, the intensities of the signal and decoy states can vary from pulse to pulse and, hence, cannot be considered constant parameters of the protocol. It can open another potential loophole and allow Eve to improve her attack strategy.

Another well-known loophole of the leaky source is the Trojan-horse attack (THA) in which Eve injects bright light pulses into Alice's device and then measures the back-reflected light in order to extract information about Alice's state preparation like the basis choice and the intensity setting in the decoy-state QKD protocol. The information leakage from Alice's IM and PM during THA is studied in Refs. [25–29]. The THA on the loss-tolerant protocol is investigated in Refs. [13,14,16,17] but only for the case of single-photon source.

In this work, we consider the most widely used two-decoy-state BB84 [23] with polarization encoding and focus on two types of source flaws—the fluctuating coherent-state intensities and the polarization misalignment due to Alice's imperfect intensity and phase modulators. We assemble a simplified optical scheme for quantum state preparation that mimics the features of realistic commercial QKD devices and extract the intensity/phase distributions from laboratory test measurements. We study the non-Poissonian photon-number statistics following Refs. [30–32] in order to take into account the fluctuating signal and decoy pulse intensities. In contrast to the model-independent analysis in [30,31], we do not rely on the knowledge of upper/lower bounds on intensities but determine the intensity probability distributions directly from the experiment. We extend this research and also investigate the imperfect encoding state preparation. Using the idea of fully-passive source [33], we compute the averaged density matrices and apply the *imbalanced quantum coin* approach [7] to estimate the phase error rate. In particular, it is demonstrated that for our setup the encoding inaccuracies can lead to the key rate reduction not exceeding 50% for channel losses up to 20 dB (equivalent to transmission distances up to 100 km), and the critical transmission distance can reach ∼120 km. Since our experimental analysis is made for illustrative purposes only, we believe that the modulation precision and data analysis can be further improved, and the key rate bound can be increased. Provided with a complete set of explicit formulas, our framework can be applied to any practical QKD system with a characterized source that implements not the loss-tolerant but the usual decoy-state BB84 protocol.

This paper is organized as follows. In Section 2, we investigate the non-Poissonian photon-number statistics of weak coherent states and estimate the effect of pulse intensity fluctuations on the secret key rate. In Section 3, we study the polarization distributions and bound the phase error rate for the QKD protocol with a realistic phase modulator. The main conclusions are given in Section 4.

2. Intensity Fluctuations

2.1. Experimental Setup

In this work, we investigate the efficient BB84 protocol [34] with non-optimized basis choice probabilities of $p_X = 0.9$ and $p_Y = 0.1$ in which the X-basis is used for the secret key distillation while the Y-basis is used for the phase error rate estimation. In order to counteract the PNS attack, we apply the three-intensity decoy-state technique [21,23]: the

signal state of intensity μ is used for the secret key generation, and two decoy states of intensities ν_1 and ν_2 are used for the single-photon yield and bit error rate estimation. For simplicity, we choose the reasonable values of $\mu \sim 0.3$, $\nu_1 \sim 0.1$ and $\nu_2 \sim 10^{-3}$ which turn out to be close to the optimal ones for a wide range of transmission distances. The states are randomly generated with the probabilities of $p_\mu = 0.5$ and $p_{\nu_{1,2}} = 0.25$.

Our experimental setup for preparing and monitoring Alice's quantum states of given intensity $\alpha \in \{\mu, \nu_1, \nu_2\}$ and polarization is presented in Figure 1. The pulses with an average optical power of approximately 2 mW are emitted by a DFB laser operating at 1550 nm wavelength. First, the relative classical pulse intensity $\mathcal{I}_\alpha$ is adjusted by the intensity modulator (IM) by applying an appropriate voltage V_α on the modulation electrodes such that $\mathcal{I}_{\nu_{1,2}}/\mathcal{I}_\mu = \nu_{1,2}/\mu$ with $\mathcal{I}_\mu$ chosen to be larger than half of the maximum output intensity. Then, the polarization state is chosen by applying one of the four voltages V_i on the phase modulator (PM). Finally, the classical pulses are attenuated to the required weak coherent-state level with the variable optical attenuator (VOA).
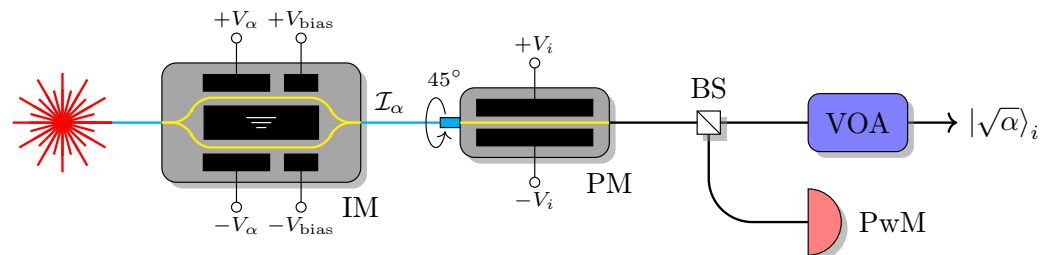

Figure 1. The optical scheme of weak coherent state preparation of given intensity and polarization: Light source—DFB laser, IM—intensity modulator Optilab IMP-1550-10-PM, PM—phase modulator IXblue MPZ-LN-10, BS—beamsplitter with the split ratio of 1:99, PwM—power meter Thorlabs PM100USB+S154C, VOA—electronic variable optical attenuator. The cyan line denotes polarization-maintaining optical fiber. The connector to PM is rotated by 45° angle with respect to the PM crystal axes.

The IM output intensity $\mathcal{I}_\alpha$ is the result of the interference of two waves, propagating via two paths of the Mach–Zehnder interferometer with different optical path lengths. This difference is created by varying the optical index in the waveguide active layer of each path with an electric field between the modulation electrodes. The IM is designed to have equal arms and thus balanced optical paths. However, there is always some imbalance, caused by the change of the refractive index of the optical mode of the waveguide due to possible variations of temperature (thermo-optic and pyroelectric effects), optical power in the waveguide (photorefractive effect) or mechanical stress (strain-optic effect). As a result, a time-dependent phase (and consequently $\mathcal{I}_\alpha$) drift is induced. In order to compensate for this drift, the time-averaged power is measured by the power meter (PwM) and tuned by the proportional–integral–derivative (PID) controller to the initial value by applying the relevant voltage V_{bias} to the bias electrodes. All these effects together with the limiting resolution of control voltage circuits and the laser noise cause some fluctuations in the output intensities.

In order to quantify the intensity fluctuations, we connect a classical photodetector (Thorlabs RXM40AF) directly to the IM output and record the voltage oscillograms. Following Ref. [35], we remove the noise by applying a filtering technique based on the singular-value-decomposition. In Figure 2, we present the obtained probability density function (PDF) of $\mathcal{I}_\alpha$ normalized by the total PM+BS+VOA attenuation. As evidenced by good agreement with the data, a regular Gaussian PDF given by Equation (1), is the right choice of function to parametrize the intensity fluctuations:

$$G(\alpha, \bar{\alpha}_i, \sigma_{\alpha_i}) = \frac{1}{\sqrt{2\pi}\sigma_{\alpha_i}} e^{-\frac{(\alpha - \bar{\alpha}_i)^2}{2\sigma_{\alpha_i}^2}}, \tag{1}$$

where $\bar{\alpha}_i$ are the mean values and σ_{α_i} are the standard deviations, with the best-fit values tabulated on the right of the plot in Figure 2.
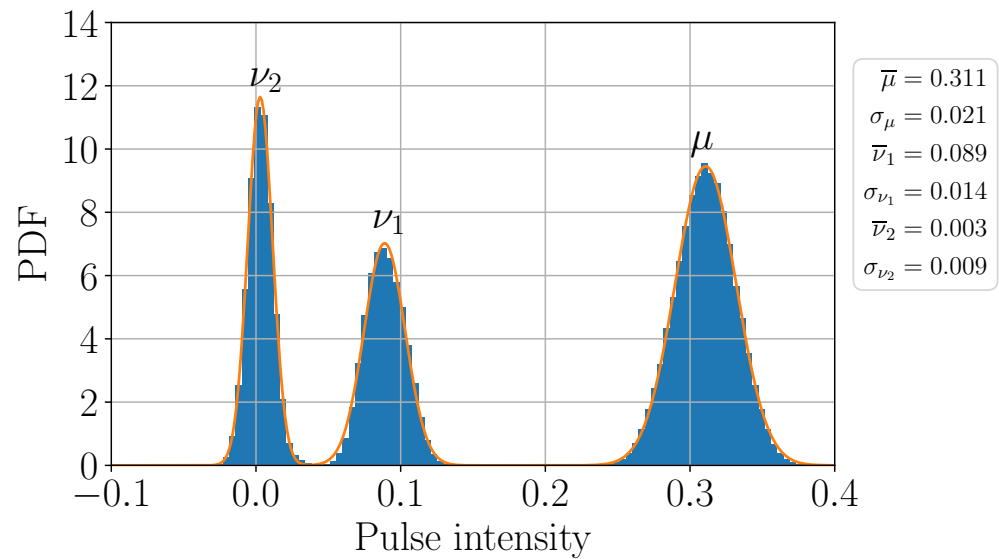

Figure 2. The measured probability density function of pulse intensity (mean photon number per pulse). The signal (μ) and two decoy ($\nu_{1,2}$) states are generated randomly with the probabilities of $p_\mu = 0.5$ and $p_{\nu_{1,2}} = 0.25$, respectively. The non-physical negative values of the vacuum decoy peak are caused by photodetector noise.

2.2. Non-Poissonian Photon-Number Statistics

The single-photon source is often approximated by a weak coherent-state source, realized in practice as strongly attenuated laser radiation. The emitted phase-randomized state is described as a mixture of Fock states,

$$\rho_\alpha = \sum_{n=0}^{\infty} P_{n|\alpha} |n\rangle\langle n| = \sum_{n=0}^{\infty} e^{-\alpha} \frac{\alpha^n}{n!} |n\rangle\langle n|, \tag{2}$$

where the photon number follows the Poisson distribution $P_{n|\alpha}$ with mean photon number α. Note that usually in the literature α is assumed to be a constant parameter that does not vary during the QKD session. However, in a realistic experimental setup, the intensity parameter is a fluctuating variable as discussed in the previous subsection.

It is known that the assumption of Poissonian photon-number statistics is not really necessary for the decoy-state BB84 protocol—one can derive the generalized security bounds for any arbitrary $P_{n|\alpha}$ distribution. The first detailed model-independent analysis of the source errors in the photon-number space is provided by Wang et al. in Refs. [30,31]. The authors derive the generalized conservative bounds on the single-photon component's yield and QBER in terms of arbitrary upper/lower bounds on $P_{n|\alpha}$. In this work, we closely follow the theoretical approach of [30,31] but do not use the bounded $P_{n|\alpha}$ that rely on the knowledge of allowed intervals $[\alpha_{\min}, \alpha_{\max}]$ for the coherent state source. Instead, we assume ρ_α of every single pulse to be Poissonian but with random normally-distributed parameter α. Thus, the n-photon state probability is modified as follows,

$$P_{n|\alpha} = \frac{\int_0^\infty e^{-\alpha} \frac{\alpha^n}{n!} G(\alpha, \bar{\alpha}, \sigma_\alpha) d\alpha}{\int_0^\infty G(\alpha, \bar{\alpha}, \sigma_\alpha) d\alpha}, \tag{3}$$

where we integrate only the positive intensity values that have physical meaning.

The experimentally measured gain—the probability that an emitted pulse of intensity α is detected by Bob—can be expressed as

$$Q_\alpha = \sum_{n=0}^{\infty} P_{n|\alpha} \mathcal{Y}_n, \tag{4}$$

where the yield $\mathcal{Y}_n$ is the conditional probability of a detection event (click) on Bob's side, given that Alice sends out an n-photon state. The key idea of the decoy-state method is that since Eve cannot distinguish the $|n\rangle$ states of signal pulse from those of decoy pulse, the yields $\{\mathcal{Y}_n\}_{n=0}^{\infty}$ must be equal for signal and decoy states [20]. However, this indistinguishability assumption may not hold in practice. In Ref. [36], the authors consider an imperfect source with passive side channels, which can partially distinguish signal and decoy states from a mismatch in such degrees of freedom as time and frequency domains. In this work, we neglect the impact of such side channels and focus only on the intensity fluctuations.

Taking into account the finite-statistics effects, the generalized lower bounds on the zero-photon and single-photon yields are determined by (for more details see Appendix A)

$$\mathcal{Y}_0^l = \max\left\{ \frac{Q_{\nu_2}^l P_{1|\nu_1} - Q_{\nu_1}^u P_{1|\nu_2}}{P_{0|\nu_2} P_{1|\nu_1} - P_{0|\nu_1} P_{1|\nu_2}}, 0 \right\}, \tag{5}$$

$$\mathcal{Y}_1^l = \frac{Q_{\nu_1}^l P_{0|\nu_2} - Q_{\nu_2}^u P_{0|\nu_1} - \dfrac{P_{2|\nu_1} P_{0|\nu_2} - P_{2|\nu_2} P_{0|\nu_1}}{P_{2|\mu}} \left(Q_\mu^u - P_{0|\mu} \mathcal{Y}_0^l \right)}{P_{0|\nu_2} P_{1|\nu_1} - P_{0|\nu_1} P_{1|\nu_2} - \dfrac{P_{2|\nu_1} P_{0|\nu_2} - P_{2|\nu_2} P_{0|\nu_1}}{P_{2|\mu}} P_{1|\mu}}. \tag{6}$$

where $Q_\alpha^{u,l}$ are the upper/lower bounds on the Q_α-estimators given by Equation (A13). For brevity, here, we omit the basis index of $Q_\alpha^{u,l}$ and $\mathcal{Y}_{0,1}^l$.

To investigate the effect of non-Poissonian statistics on the privacy amplification, in Figure 3 we plot the simulated ratio of the secret over verified key lengths, $\ell_{\text{sec}}/\ell_{\text{ver}}$, as a function of transmission distances for the scenarios of perfect (Poissonian statistics with $P_{n|\alpha} = e^{-\bar{\alpha}} \bar{\alpha}^n / n!$) and imperfect (non-Poissonian statistics with $P_{n|\alpha}$ defined by Equation (3)) intensity modulation. The verified key is the error-corrected sifted key that passed the subsequent hash-tag verification. The secret key length formula is given in Appendix B. Here, we assume the photon source to be basis-independent ($\Delta' = 0$ in Equation (A16)). One can see from the plot that, surprisingly, the imperfect preparation provides a better key rate than the perfect one for the entire distance range. The reason is the following: due to rather wide distribution of ν_2 relative to its mean value, the probability of the single-photon component of ρ_{ν_2} turns out to be enhanced several times with respect to the ideal Poissonian source with the mean photon number $\bar{\nu}_2$; as a consequence, the term $P_{0|\nu_1} P_{1|\nu_2}$ in the denominator of Equation (6) becomes non-negligible, which, in turn, increases $\mathcal{Y}_1^l$ and, hence, ℓ_{sec}. One could naively think that increasing σ_{ν_2} would improve ℓ_{sec} even more; however, this would lead to the violation of the required condition (A2) starting from some value of n, making the $\mathcal{Y}_0$-estimation (A1) incorrect. Increasing σ_{ν_2}, e.g., by 5 times would violate (A2) for $n \geq 12$. In order to avoid the overestimation of the single-photon and multi-photon contributions to ρ_{ν_2} due to the noise, we propose to set $P_{0|\nu_2} = 1$ and $P_{n \geq 1|\nu_2} = 0$ (i.e., $\nu_2 \equiv 0$), which provides a more conservative evaluation of ℓ_{sec} (see the green curve in Figure 3). In this case, the secret key turns out to be more than 95% of the key generated with an ideal IM, for any distance up to 100 km.
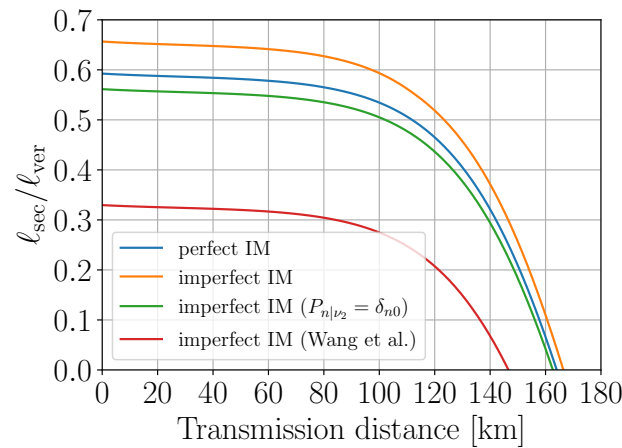
Figure 3. The simulated secret key length ℓ_{sec}, normalized to the verified key length ℓ_{ver}, for the scenarios of perfect (μ, ν_1, ν_2 are constant) and imperfect (μ, ν_1, ν_2 fluctuate following the normal distribution) pulse intensity modulation. The red curve represents the result of the method introduced by Wang et al. in [30,31] with the intensities bounded with their $\pm 1\sigma$ uncertainties.

To conclude this section, we make a comparison with the model-independent approach of Wang et al. [30,31]. The single-photon gain is given by Equation (43) in Ref. [31] which can be written in our notations as

$$Q_1^l = P_{1|\mu}^l \mathcal{Y}_1^l = P_{1|\mu}^l \frac{Q_{\nu_1}^l P_{2|\mu}^l - Q_\mu^u P_{2|\nu_1}^u - \left(P_{2|\mu}^l P_{0|\nu_1}^u - P_{2|\nu_1}^u P_{0|\mu}^l\right) \frac{Q_{\nu_2}^u}{P_{0|\nu_2}^l}}{P_{2|\mu}^l P_{1|\nu_1}^u - P_{2|\nu_1}^u P_{1|\mu}^l}, \tag{7}$$

with bounded probabilities for coherent states defined as

$$P_{n|\alpha}^{u(l)} = \begin{cases} e^{-\alpha^{l(u)}}, & n = 0 \\ \frac{\left(\alpha^{u(l)}\right)^n}{n!} e^{-\alpha^{u(l)}}, & n = 1, 2 \end{cases} \tag{8}$$

Using the experimental intensity distributions in Figure 2 we determine $\alpha^{u,l}$ as

$$\alpha^{u(l)} = \bar{\alpha} \pm z_{1-\varepsilon} \sigma_\alpha, \quad \Pr(\alpha \le \alpha^l) = \Pr(\alpha \ge \alpha^u) = \varepsilon, \tag{9}$$

where $z_{1-\varepsilon}$ is the normal distribution quantile,

$$z_{1-\varepsilon} = \Phi^{-1}(1-\varepsilon) = \sqrt{2}\,\text{erf}^{-1}(1-2\varepsilon). \tag{10}$$

For illustration, the red curve in Figure 3 represents the normalized secret key length (A11) computed with Q_1^l defined by Equation (7) and $z_{1-\varepsilon} = 1$ ($\varepsilon \simeq 0.16$). We find that for $z_{1-\varepsilon} \gtrsim 2.3$ ($\varepsilon \lesssim 0.011$) the secret key transmission is impossible at any distance. One can clearly see superiority of the proposed method for the particular setup and measurement precision since it provides larger key length and the maximum attainable transmission distance.

3. Phase Fluctuations

3.1. Polarization State Preparation and Basis-Dependence

Any arbitrary polarization state can be described by azimuthal and polar angles $\varphi \in [0, 2\pi)$ and $\theta \in [0, \pi]$ on the Bloch sphere,

$$|\psi(\varphi, \theta)\rangle = \cos\left(\frac{\theta}{2}\right)|H\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|V\rangle, \tag{11}$$

where $|H\rangle$ and $|V\rangle$ denote the horizontal and vertical polarization vectors, aligned with the PM crystal axes. In our setup, the linearly polarized light is injected to PM at a 45° angle to the crystal axes, which corresponds to $\theta = \pi/2$ [37]. In general, the electric field amplitudes along the ordinary and extraordinary axes initially have some phase difference ϕ_0 without any voltage supply due to the crystal birefringence. The additional random relative phase $\phi_i \in \{0, \pi, \pi/2, 3\pi/2\}$, determining the basis and bit value, is created by applying an appropriate voltage V_i along one of the crystal axes. Thus, the azimuthal angle of the ith state is $\varphi_i = \phi_0 + \phi_i$.

In the protocol with perfect state preparation, the qubits are prepared and measured in the elliptical polarization bases $X' : \{|\psi_1\rangle, |\psi_2\rangle\}$ and $Y' : \{|\psi_3\rangle, |\psi_4\rangle\}$, obtained by rotating the standard bases $X : \{|D\rangle, |A\rangle\}$ and $Y : \{|R\rangle, |L\rangle\}$ around the z-axis by ϕ_0 (see Figure 4), with the basis vectors in the form of

$$|\psi_{1,2}^{\text{perfect}}\rangle = \frac{1}{\sqrt{2}} \big(|H\rangle \pm e^{i\phi_0} |V\rangle \big), \quad |\psi_{3,4}^{\text{perfect}}\rangle = \frac{1}{\sqrt{2}} \big(|H\rangle \pm i e^{i\phi_0} |V\rangle \big). \tag{12}$$

Then, Bob performs his measurement in the X' and Y' bases by randomly applying one of the positive operator-valued measures $\{|\psi_i^{\text{perfect}}\rangle\langle\psi_i^{\text{perfect}}|\}$.

However, in practice, the light enters PM not ideally at 45° due to mechanical inaccuracy of connection between the optical components. This error induces a deviation from $\theta = \pi/2$ on the Bloch sphere. The voltage control and, hence, $\{\phi_i\}$ have some uncertainty as well. As a consequence of all these imperfections, the ideal states (12) float above/below the xy-plane and rotate around the z-axis, fluctuating around their average positions. So, the physical states sent to Bob can be written as:

$$|\psi_i\rangle = |\psi(\varphi_i, \theta)\rangle, \tag{13}$$

where φ_i is a random variable with some probability distribution while θ is an *a priori* unknown that is determined from experiments with some uncertainty. Note that, in general, these states are no longer mutually orthogonal in the corresponding basis and do not lie in the xy-plane.
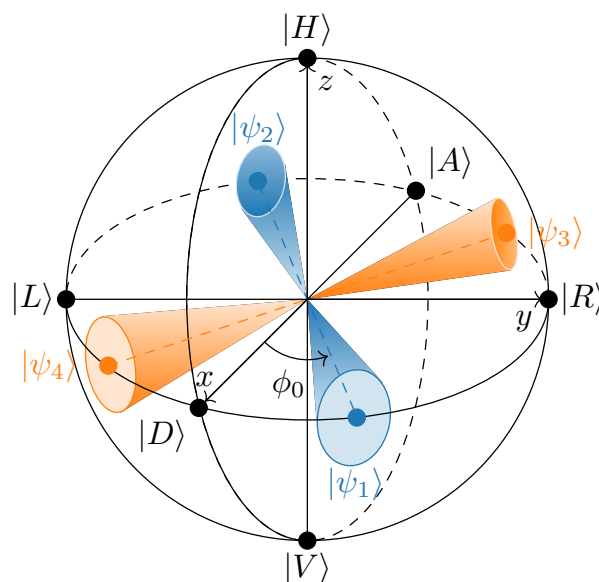

Figure 4. Alice's output polarization states on the Bloch sphere. The blue and orange dots mark the perfectly prepared states (12), while the realistic states (13) are schematically depicted as solid angle surface areas.

Using the density matrix formalism, the X'-basis and Y'-basis states are described by $\rho_{X'} = \frac{1}{2}(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|)$ and $\rho_{Y'} = \frac{1}{2}(|\psi_3\rangle\langle\psi_3| + |\psi_4\rangle\langle\psi_4|)$ that can be written as

$$
\begin{aligned}
\rho_{X'} &= \frac{1}{2}\begin{pmatrix} 1 + \cos\theta & e^{-i\frac{\varphi_1+\varphi_2}{2}}\cos\left(\frac{\varphi_1-\varphi_2}{2}\right)\sin\theta \\ e^{i\frac{\varphi_1+\varphi_2}{2}}\cos\left(\frac{\varphi_1-\varphi_2}{2}\right)\sin\theta & 1 - \cos\theta \end{pmatrix}, \\
\rho_{Y'} &= \frac{1}{2}\begin{pmatrix} 1 + \cos\theta & e^{-i\frac{\varphi_3+\varphi_4}{2}}\cos\left(\frac{\varphi_3-\varphi_4}{2}\right)\sin\theta \\ e^{i\frac{\varphi_3+\varphi_4}{2}}\cos\left(\frac{\varphi_3-\varphi_4}{2}\right)\sin\theta & 1 - \cos\theta \end{pmatrix}.
\end{aligned}
\tag{14}
$$

For the perfectly prepared states (12) $\rho_{X'} = \rho_{Y'}$, i.e., the photon source is basis-independent. If $\rho_{X'} \neq \rho_{Y'}$, one cannot simply estimate the unknown single-photon phase error rate in the X'-basis $E_1^{\mathrm{ph},X'}$ by the measured bit error rate in the Y'-basis $E_1^{Y'}$ (or vice versa). The more state dependence on the basis, the easier for Eve to distinguish the bases and hence the lower secret key rate.

In Ref. [33], dedicated to the fully-passive QKD, the authors consider an equivalent virtual entanglement-based protocol with a source that emits perfectly encoded pure decoy states in the X, Y-bases and signal states with mixed polarizations in the Z-basis. It is shown that Alice's imperfect preparation in the Z-basis is equivalent to the imperfect measurement (i.e., the trusted noise in Alice's post-processing) and does not affect the amount of privacy amplification. However, the authors make an assumption that the polarization fluctuations in the Z-basis are symmetric on the Bloch sphere. It implies that averaged over angles ρ_Z is the fully-mixed state, i.e., $\bar{\rho}_H + \bar{\rho}_V = \mathbb{I}$ where

$$
\begin{aligned}
\bar{\rho}_H &= \int_0^{2\pi}\int_0^{\delta\theta} p(\varphi,\theta)\,|\psi(\varphi,\theta)\rangle\langle\psi(\varphi,\theta)|\,d\varphi d\theta, \\
\bar{\rho}_V &= \int_0^{2\pi}\int_{\pi-\delta\theta}^{\pi} p(\varphi,\theta)\,|\psi(\varphi,\theta)\rangle\langle\psi(\varphi,\theta)|\,d\varphi d\theta,
\end{aligned}
\tag{15}
$$

are the mixed states, post-selected within two cones around the z-axis with half-angle $\delta\theta$, with symmetric probability distribution $p(\varphi,\theta) = p(\varphi + \pi, \theta)$.

This approach is not applicable in our case since we do not assume any symmetry of angular probability distributions $\{p_i(\varphi,\theta)\}$. Nevertheless, we can use one of the ideas of Refs. [33,38]—the replacement of the source of randomly fluctuating pure states $\{|\psi_i\rangle\}$ by an equivalent source emitting the mixed states $\{\bar{\rho}_i\}$,

$$
\bar{\rho}_i = \int_0^{2\pi}\int_0^{\pi} p_i(\varphi,\theta)\,|\psi(\varphi,\theta)\rangle\langle\psi(\varphi,\theta)|\,d\varphi d\theta,
\tag{16}
$$

where $\{p_i(\varphi,\theta)\}$ are extracted directly from experiment. In this case, the density matrices (14) are substituted for

$$
\bar{\rho}_{X'} = \bar{\rho}_1 + \bar{\rho}_2, \quad \bar{\rho}_{Y'} = \bar{\rho}_3 + \bar{\rho}_4.
\tag{17}
$$

To quantify the discrepancy between $E_1^{\mathrm{ph},X'}$ and $E_1^{Y'}$, we use the concept of *quantum coin*, introduced in Ref. [7] in the equivalent virtual entanglement-based protocol in which both Alice and Bob measure in one basis and Alice announces the other basis. Applying the complementarity argument [6] and the Bloch sphere bound [39] to the quantum coin yields the following inequality [40],

$$
\sqrt{F(\bar{\rho}_{X'}, \bar{\rho}_{Y'})} \leq 1 - \mathcal{Y}_1 + \mathcal{Y}_1\left(\sqrt{E_1^{\mathrm{ph},X'}E_1^{Y'}} + \sqrt{(1 - E_1^{\mathrm{ph},X'})(1 - E_1^{Y'})}\right),
\tag{18}
$$

with $\mathcal{Y}_1 = (\mathcal{Y}_1^{X'} + \mathcal{Y}_1^{Y'})/2$ and *fidelity F* between two states, defined as

$$
F(\bar{\rho}_{X'}, \bar{\rho}_{Y'}) \equiv \left[\mathrm{Tr}\left(\sqrt{\sqrt{\bar{\rho}_{X'}}\,\bar{\rho}_{Y'}\,\sqrt{\bar{\rho}_{X'}}}\right)\right]^2.
\tag{19}
$$

For 2×2 matrices, it is more convenient to use the simplified form [41],

$$F(\bar{\rho}_{X'}, \bar{\rho}_{Y'}) = \text{Tr}(\bar{\rho}_{X'}\,\bar{\rho}_{Y'}) + 2\sqrt{\det(\bar{\rho}_{X'})\det(\bar{\rho}_{Y'})}. \tag{20}$$

Solving (18), one obtains the following upper bound on the single-photon phase error rate,

$$E_1^{\text{ph},X'} \le E_1^{Y'} + 4\Delta'(1 - \Delta')(1 - 2E_1^{Y'}) + 4(1 - 2\Delta')\sqrt{\Delta'(1 - \Delta')E_1^{Y'}(1 - E_1^{Y'})}, \tag{21}$$

$$\Delta' = \frac{1 - \sqrt{F(\bar{\rho}_{X'}, \bar{\rho}_{Y'})}}{2\mathcal{Y}_1} = \frac{\Delta}{\mathcal{Y}_1}, \tag{22}$$

where the quantity of $\Delta = (1 - \sqrt{F})/2$ is usually called the *quantum coin imbalance*. The lower and upper bounds on $\mathcal{Y}_1^{X',Y'}$ and $E_1^{Y'}$ are determined via the decoy-state method and are given by Equations (6) and (A20), respectively. The finite-key-size effects are taken into account in the modified $E_1^{\text{ph},X'}$ Formula (A15).

3.2. Experimental Data Analysis

Using the optical scheme shown in Figure 1, we perform a series of polarization state measurements with the fast polarimeter (model PSY-201 by General Photonics). A periodic sequence of repeated constant voltage pulses corresponding to the phase retardation angles of $\{0, \pi/2, \pi, 3\pi/2\}$ is applied to the phase modulator. The time duration of each pulse is $\sim 52\,\mu\text{s}$. A representative result of such polarization measurements in terms of three-component Stokes vector (S_1, S_2, S_3) is shown in Figure 5. One can see that the data points form a ring that is slightly shifted below the primary xy-plane of the Poincaré sphere. The majority of individual data points are grouped into four primary spots that are turned on that ring at an angle of $\phi_0 \sim 60°$ around the z-axis of the sphere (see Figure 5, right panel). Sparse points between the primary four dense regions are artifacts of not high enough acquisition rate of the polarimeter.
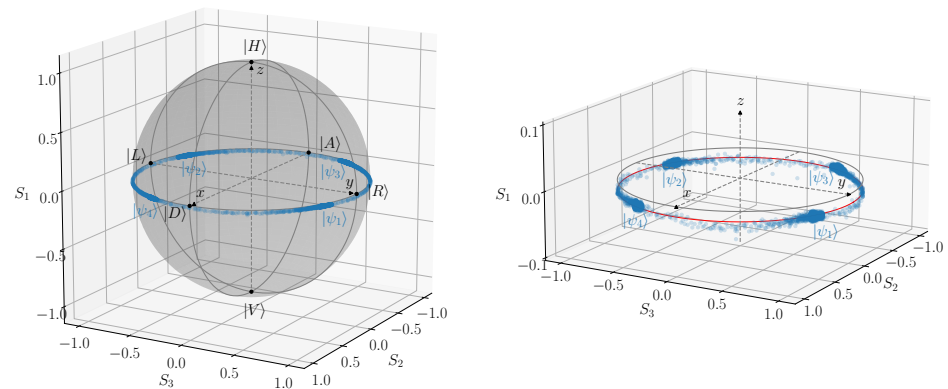

Figure 5. The measured polarization states (13) on the Poincaré sphere, made in the Stokes parameter coordinates (S_1, S_2, S_3). The plot on the right shows the zoomed equatorial area of the sphere. The red circle is the best-fit circle given 3D points.

The typical experimental distributions of azimuthal (φ) and polar (θ) angles,

$$\varphi = \text{sgn}(S_3)\arccos\frac{S_2}{\sqrt{S_2^2 + S_3^2}}, \quad \theta = \arccos\frac{S_1}{\sqrt{S_1^2 + S_2^2 + S_3^2}}, \tag{23}$$

are presented in Figure 6. One can notice that the φ_i—distributions are clearly asymmetric; however, the study of this asymmetry origin is beyond the scope of this work. Therefore, first, we make a conservative estimation of Δ using the model-independent approach: we

extract the experimental normalized binned PDFs $p_{\varphi_i}^{\exp}$ and $p_\theta^{\exp}$ from Figure 6 and compute $\bar{\rho}_i$ as follows,

$$\bar{\rho}_i = \sum_{n,m} p_{\varphi_i}^{\exp}(\varphi_i^{\text{bin }n}) p_\theta^{\exp}(\theta^{\text{bin }m}) |\psi(\varphi_i^{\text{bin }n}, \theta^{\text{bin }m})\rangle\langle\psi(\varphi_i^{\text{bin }n}, \theta^{\text{bin }m})| w_{\varphi_i} w_\theta, \qquad (24)$$

where $x^{\text{bin }n}$ is the center of nth histogram bin of width w_x of measured x-distribution ($x \in \{\varphi_i, \theta\}$). Then, for the density matrices computed in this way, we obtain $\Delta = 7 \times 10^{-6}$. In Figure 7, we plot the privacy amplification factor $\ell_{\sec}/\ell_{\text{ver}}$ where $\ell_{\sec}$ is determined by Equation (A11) with corrected single-photon phase error rate (21). Here, we assume no intensity fluctuations (i.e., $P_{n|\alpha} = e^{-\bar{\alpha}} \bar{\alpha}^n / n!$ and $\mathcal{Y}_{0,1}^l$ are determined by Equations (A7) and (A8)). One can see from the plot that the critical distance at which the secret key generation becomes impossible is reduced by approximately 40 km with respect to the perfect phase modulation case. One can also remark that the secret key rate reduction is up to 9 and 47% for the short-distance (up to 50 km) and long-distance (up to 100 km) ranges, respectively.

We assume that increasing the data statistics and improving the measurement procedure with subsequent data post-processing will make the distributions smoother and symmetric. Applying a simple Gaussian model, we obtain for future prospects the following analytical approximation (verified by numerical integration),

$$\begin{aligned} \bar{\rho}_i &\simeq \int_0^{2\pi} \int_0^\pi G(\varphi, \bar{\varphi}_i, \sigma_{\varphi_i}) G(\theta, \bar{\theta}, \sigma_\theta) |\psi(\varphi, \theta)\rangle\langle\psi(\varphi, \theta)| \, d\varphi d\theta \\ &\simeq \frac{1}{2} \begin{pmatrix} 1 + e^{-\frac{\sigma_\theta^2}{2}} \cos\bar{\theta} & e^{-i\bar{\varphi}_i - \frac{1}{2}(\sigma_{\varphi_i}^2 + \sigma_\theta^2)} \sin\bar{\theta} \\ e^{i\bar{\varphi}_i - \frac{1}{2}(\sigma_{\varphi_i}^2 + \sigma_\theta^2)} \sin\bar{\theta} & 1 - e^{-\frac{\sigma_\theta^2}{2}} \cos\bar{\theta} \end{pmatrix}, \end{aligned} \qquad (25)$$

where, for simplicity, we omit the properly defined PDF normalization factors since

$$\int_0^{x_{\max}} G(x, \bar{x}, \sigma_x) dx = \frac{1}{2}\left[\text{erf}\left(\frac{\bar{x}}{\sqrt{2}\sigma}\right) + \text{erf}\left(\frac{x_{\max} - \bar{x}}{\sqrt{2}\sigma}\right)\right] \simeq 1, \qquad (26)$$

if $\sigma_x \ll \bar{x}$ and $\sigma_x \ll x_{\max} - \bar{x}$. For the same reason, we replace the integration limits in (25) by $\pm\infty$ and obtain a very simple analytical matrix expression above. Using the fitted parameter values of $\{\bar{\varphi}_i, \sigma_{\varphi_i}, \bar{\theta}, \sigma_\theta\}$ from Figure 6, we compute the fidelity between $\bar{\rho}_{X'}$ and $\bar{\rho}_{Y'}$ (19) and find $\Delta = 3 \times 10^{-6}$. One can see from the plot in Figure 7 that the critical distance is reduced by approximately 30 km compared to the ideal modulation case. Also, one can note that for the short(long)-distance range the secret key length is reduced by less than 5 (27)%. These results turn out to be less conservative than those obtained with the model-independent approach, providing better secret key generation rate.
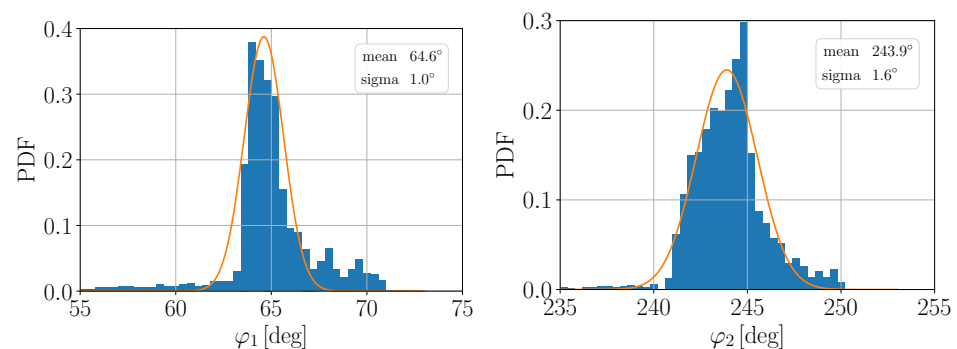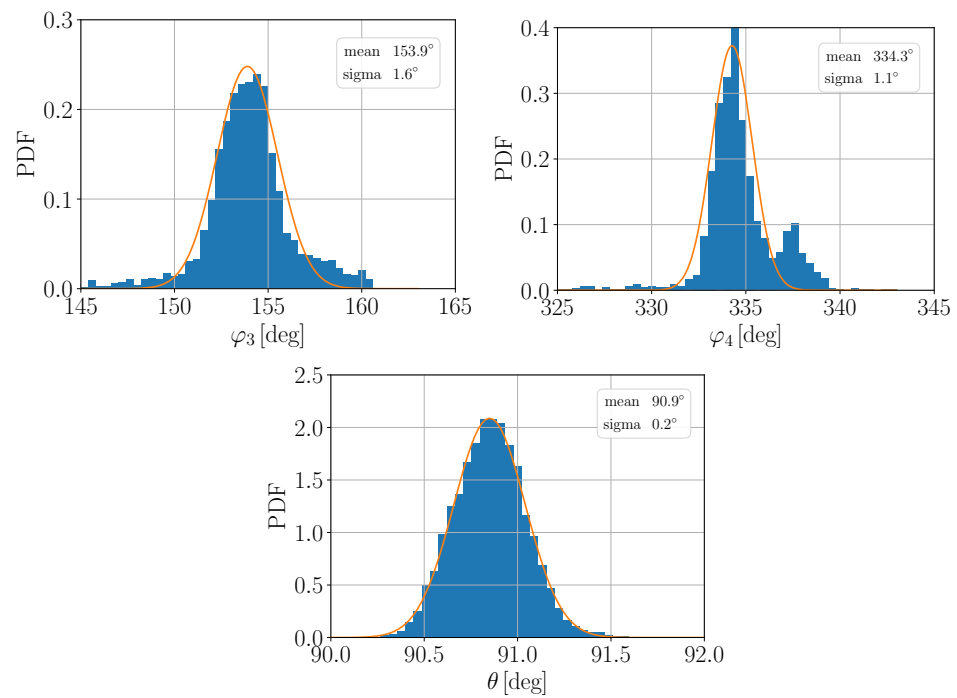

Figure 6. *Cont.*

Figure 6. The experimental angular distributions, obtained from the spherical coordinates of the data points on the Poincaré sphere in Figure 4.
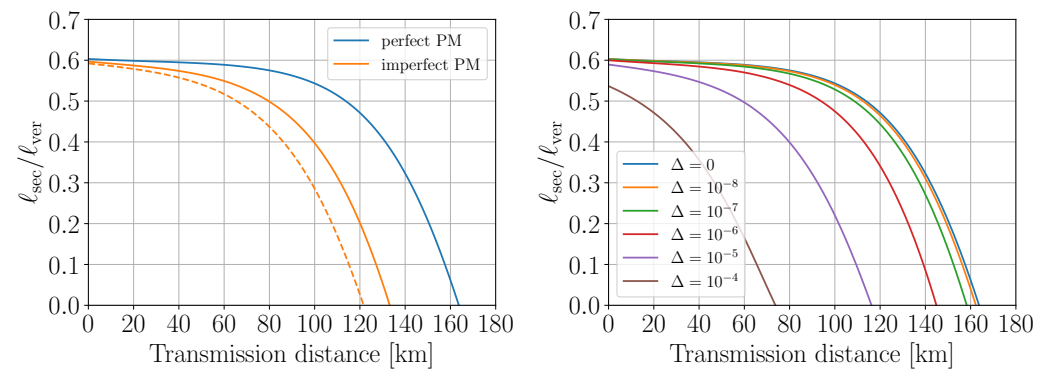

Figure 7. (**Left**): The simulated secret key length ℓ_{sec}, normalized to the verified key length ℓ_{ver}, for scenarios of perfect and imperfect phase modulation. The orange solid (dashed) line corresponds to the fitted Gaussian (experimental binned) probability density function of angular distributions. (**Right**): The simulated $\ell_{\text{sec}}/\ell_{\text{ver}}$ ratio for various values of quantum coin imbalance Δ.

Finally, we also compare with a very conservative estimation of Δ by finding the minimum of fidelity (i.e., maximum of Δ),

$$
\begin{aligned}
F_{\min} = \min_{\substack{\varphi_i \in [\varphi_i^{\min}, \varphi_i^{\max}] \\ \theta \in [\theta^{\min}, \theta^{\max}]}} F(\rho_{X'}, \rho_{Y'}) &= \min_{\substack{\varphi_i \in [\varphi_i^{\min}, \varphi_i^{\max}] \\ \theta \in [\theta^{\min}, \theta^{\max}]}} \frac{1}{2} \Bigg\{ 1 + \cos^2 \theta \\
&+ \cos\left(\frac{\varphi_1 + \varphi_2 - \varphi_3 - \varphi_4}{2}\right) \cos\left(\frac{\varphi_1 - \varphi_2}{2}\right) \cos\left(\frac{\varphi_3 - \varphi_4}{2}\right) \sin^2 \theta \\
&+ \left| \sin\left(\frac{\varphi_1 - \varphi_2}{2}\right) \sin\left(\frac{\varphi_3 - \varphi_4}{2}\right) \right| \sin^2 \theta \Bigg\},
\end{aligned}
\tag{27}
$$

with $\rho_{X'}$ and $\rho_{Y'}$, defined by Equation (14). The minimization ranges are determined from the experimental distributions in Figure 6 as, e.g., 90% confidence intervals. One can show that the minimum is achieved for the values of θ closest to $\pi/2$ and for at least one

of the four combinations of $\varphi_{1,3} = \varphi_{1,3}^{\min(\max)}$ and $\varphi_{2,4} = \varphi_{2,4}^{\max(\min)}$ since they minimize the last $\sin^2\theta$-term which is dominant for $\theta \sim \pi/2$ and $\varphi_{2(4)} - \varphi_{1(3)} \sim \pi$. This yields $F_{\min} = 0.9975$ and $\Delta_{\max} = (1 - \sqrt{F_{\min}})/2 = 6 \times 10^{-4}$. In this case, the critical transmission distance is limited to 40 km, and the maximum ℓ_{sec}/ℓ_{ver} ratio is about 0.4 at zero loss. A similar estimation of F and Δ using the upper-bounded phase modulation errors is made in the GLLP security analysis for the phase-encoding decoy-state BB84 with source flaws in Ref. [9]. For completeness, on the right-hand side of Figure 7 we plot the ℓ_{sec}/ℓ_{ver} ratio for various Δ-values, from which one can see that $\Delta \lesssim 10^{-8}$ is required in order to make the basis-dependence effect negligible.

4. Discussion

In this work, we study the security of practical efficient decoy-state BB84 QKD protocol with polarization encoding accounting for the source flaws due to imperfect intensity and phase modulation. Based on our experimental data, we use the normal distribution to describe the non-Poissonian photon-number statistics and derive the generalized bounds on zero/single-photon yields. We find that the effect of intensity fluctuations on the secret key length is less than 5% for any transmission distances up to 100 km. It is also demonstrated that for our experimental setup, the proposed method turns out to be less conservative than the one introduced in Refs. [30,31]. In order to take into account the imperfect polarization state preparation, we apply an idea from the fully-passive source approach [38] and compute the density matrices of mixed states in two polarization bases; then we evaluate the fidelity between them and estimate the upper bound on the phase error rate using the concept of imbalanced quantum coin [6,7,40]. From the analysis of experimental angular distributions, we find that the key length is reduced by less than 9 and 47% for the transmission distances up to 50 and 100 km, respectively. The maximum distance at which the secret key transmission becomes impossible is reduced from 160 km to 120 km when the phase modulation uncertainties are taken into account. The proposed approach of estimating the fidelity between the mixed states turns out to be significantly better than the more conservative evaluation by minimizing the fidelity of pure states (e.g., compare the maximum distance of 120 km versus 40 km). We emphasize that these results are preliminary. The fidelity estimation could be further improved in our future work by (i) enlarging the amount of data for the statistical analysis (we have just ∼2500 data points for each polarization state), (ii) improving the voltage and temperature control, (iii) applying a more advanced post-selection procedure for the polarimeter data, (iv) performing a more sophisticated angular analysis. Although the obtained numerical results are valid only for the particular simple optical layout that mimics a realistic QKD transmitter, the explicit analytical formulas of the present approach can be readily applied to any practical implementation of the widely-used two-decoy-state BB84 QKD protocol with imperfect quantum state preparation augmented with the relevant source characterization data.

Author Contributions: Conceptualization, A.R. and A.T.; methodology, A.R., A.T., V.M. and O.F.; visualization, A.R. and A.T.; investigation, A.R. and A.T.; experiment and data acquisition, V.M. and O.F.; validation, A.R., A.T., V.M. and O.F.; writing—original draft preparation, A.R. and A.T.; writing—review and editing, A.T., V.M. and O.F.; project administration and supervision, A.T.; funding acquisition, A.T. All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

QKD   Quantum Key Distribution
BB84   QKD protocol developed by Bennett and Brassard in 1984
GLLP   Gottesman, Lo, Lütkenhaus, Preskill
EPR   Einstein, Podolsky, Rosen
IM   Intensity Modulator
PM   Phase Modulator
PDF   Probability Density Function

Appendix A. Generalized Bounds on $\mathcal{Y}_{0,1}$

Following the procedure for classical Poissonian source in Ref. [23], one can write

$$
\begin{aligned}
Q_{\nu_2} P_{1|\nu_1} - Q_{\nu_1} P_{1|\nu_2} &= (P_{0|\nu_2} P_{1|\nu_1} - P_{0|\nu_1} P_{1|\nu_2}) \mathcal{Y}_0 \\
&+ \sum_{n=2}^{\infty} (P_{n|\nu_2} P_{1|\nu_1} - P_{n|\nu_1} P_{1|\nu_2}) \mathcal{Y}_n \\
&\leq (P_{0|\nu_2} P_{1|\nu_1} - P_{0|\nu_1} P_{1|\nu_2}) \mathcal{Y}_0,
\end{aligned} \tag{A1}
$$

where the inequality follows from the required condition

$$
P_{n|\nu_2} P_{1|\nu_1} - P_{n|\nu_1} P_{1|\nu_2} = \iint_0^\infty e^{-\nu_1 - \nu_2} \frac{\nu_1 \nu_2}{n!} (\nu_2^{n-1} - \nu_1^{n-1}) G_{\nu_1} G_{\nu_2} d\nu_1 d\nu_2 \overset{n \geq 2}{<} 0. \tag{A2}
$$

Here, for short, we use the notation $G_\alpha \equiv G(\alpha, \bar{\alpha}, \sigma_\alpha) / \int_0^\infty G(\alpha, \bar{\alpha}, \sigma_\alpha) d\alpha$. Thus, the modified lower bound on $\mathcal{Y}_0$ is given by

$$
\mathcal{Y}_0 \geq \mathcal{Y}_0^l = \max \left\{ \frac{Q_{\nu_2} P_{1|\nu_1} - Q_{\nu_1} P_{1|\nu_2}}{P_{0|\nu_2} P_{1|\nu_1} - P_{0|\nu_1} P_{1|\nu_2}}, 0 \right\}. \tag{A3}
$$

Writing another combination of gains, one obtains

$$
\begin{aligned}
Q_{\nu_1} P_{0|\nu_2} - Q_{\nu_2} P_{0|\nu_1} &= (P_{1|\nu_1} P_{0|\nu_2} - P_{1|\nu_2} P_{0|\nu_1}) \mathcal{Y}_1 \\
&+ \sum_{n=2}^{\infty} (P_{n|\nu_1} P_{0|\nu_2} - P_{n|\nu_2} P_{0|\nu_1}) \mathcal{Y}_n \\
&\leq (P_{1|\nu_1} P_{0|\nu_2} - P_{1|\nu_2} P_{0|\nu_1}) \mathcal{Y}_1 \\
&+ \frac{P_{2|\nu_1} P_{0|\nu_2} - P_{2|\nu_2} P_{0|\nu_1}}{P_{2|\mu}} \sum_{n=2}^{\infty} P_{n|\mu} \mathcal{Y}_n \\
&= (P_{1|\nu_1} P_{0|\nu_2} - P_{1|\nu_2} P_{0|\nu_1}) \mathcal{Y}_1 \\
&+ \frac{P_{2|\nu_1} P_{0|\nu_2} - P_{2|\nu_2} P_{0|\nu_1}}{P_{2|\mu}} (Q_\mu - P_{0|\mu} \mathcal{Y}_0 - P_{1|\mu} \mathcal{Y}_1),
\end{aligned} \tag{A4}
$$

where the inequality follows from another required condition,

$$
\begin{aligned}
&P_{n|\mu} (P_{2|\nu_1} P_{0|\nu_2} - P_{2|\nu_2} P_{0|\nu_1}) - P_{2|\mu} (P_{n|\nu_1} P_{0|\nu_2} - P_{n|\nu_2} P_{0|\nu_1}) \\
&= \iiint_0^\infty e^{-\mu - \nu_1 - \nu_2} \frac{\mu^{n+2}}{2! n!} \left[\frac{\nu_1^2}{\mu^2} - \frac{\nu_2^2}{\mu^2} - \left(\frac{\nu_1^n}{\mu^n} - \frac{\nu_2^n}{\mu^n} \right) \right] G_\mu G_{\nu_1} G_{\nu_2} d\mu d\nu_1 d\nu_2 \overset{n \geq 2}{\geq} 0.
\end{aligned} \tag{A5}
$$

As a result, the lower bound on the single-photon yield is given by

$$\mathcal{Y}_1 \geq \mathcal{Y}_1^l = \frac{Q_{\nu_1}P_{0|\nu_2} - Q_{\nu_2}P_{0|\nu_1} - \dfrac{P_{2|\nu_1}P_{0|\nu_2} - P_{2|\nu_2}P_{0|\nu_1}}{P_{2|\mu}}(Q_\mu - P_{0|\mu}\mathcal{Y}_0^l)}{P_{1|\nu_1}P_{0|\nu_2} - P_{1|\nu_2}P_{0|\nu_1} - \dfrac{P_{2|\nu_1}P_{0|\nu_2} - P_{2|\nu_2}P_{0|\nu_1}}{P_{2|\mu}}P_{1|\mu}}. \tag{A6}$$

Substituting $P_{n|\alpha} \to e^{-\bar{\alpha}}\bar{\alpha}^n/n!$ in Equations (A3) and (A6), one easily recovers the "classic" yield expressions for a perfect Poissonian source [23],

$$\mathcal{Y}_0^l = \max\left\{\frac{\bar{\nu}_1 Q_{\nu_2}e^{\bar{\nu}_2} - \bar{\nu}_2 Q_{\nu_1}e^{\bar{\nu}_1}}{\bar{\nu}_1 - \bar{\nu}_2}, 0\right\}, \tag{A7}$$

$$\mathcal{Y}_1^l = \frac{\bar{\mu}}{(\bar{\nu}_1 - \bar{\nu}_2)(\bar{\mu} - \bar{\nu}_1 - \bar{\nu}_2)}\left[Q_{\nu_1}e^{\bar{\nu}_1} - Q_{\nu_2}e^{\bar{\nu}_2} - \frac{\bar{\nu}_1^2 - \bar{\nu}_2^2}{\bar{\mu}^2}(Q_\mu e^{\bar{\mu}} - \mathcal{Y}_0^l)\right]. \tag{A8}$$

Also, imposing $P_{0|\nu_2} = 1$, $P_{n|\nu_1} = 0$ and $P_{2|\nu_1}/P_{2|\mu} \geq P_{n|\nu_1}/P_{n|\mu}$ for $n \geq 2$, we recover the result of Ref. [32].

Note that $\{\mu, \nu_1, \nu_2\}$ are random variables, and, hence, one cannot justify the inequalities (A2) and (A5) analytically by simply imposing the constraints $\nu_2 < \nu_1$ and $\nu_1 + \nu_2 < \mu$, as was performed in Ref. [23]. Therefore, we verify them numerically by computing the integrals in terms of special functions. For completeness, we present $P_{n|\alpha}$ (3) for $n = 0, 1, 2$ expressed in terms of the error function:

$$P_{0|\alpha} = e^{-\bar{\alpha}+\frac{\sigma_\alpha^2}{2}}\left[1 - \operatorname{erf}\left(-\frac{\bar{\alpha} - \sigma_\alpha^2}{\sqrt{2}\sigma_\alpha}\right)\right]\left[1 + \operatorname{erf}\left(\frac{\bar{\alpha}}{\sqrt{2}\sigma_\alpha}\right)\right]^{-1},$$

$$P_{1|\alpha} = \frac{e^{-\frac{\bar{\alpha}^2}{2\sigma_\alpha^2}}}{\sqrt{2\pi}}\left\{2\sigma_\alpha + \sqrt{2\pi}e^{\frac{(\bar{\alpha}-\sigma_\alpha^2)^2}{2\sigma_\alpha^2}}(\bar{\alpha} - \sigma_\alpha^2)\left[1 + \operatorname{erf}\left(\frac{\bar{\alpha} - \sigma_\alpha^2}{\sqrt{2}\sigma_\alpha}\right)\right]\right\}$$

$$\times \left[1 + \operatorname{erf}\left(\frac{\bar{\alpha}}{\sqrt{2}\sigma_\alpha}\right)\right]^{-1}, \tag{A9}$$

$$P_{2|\alpha} = \frac{e^{-\frac{\bar{\alpha}^2}{2\sigma_\alpha^2}}}{2\sqrt{2\pi}}\left\{2\sigma_\alpha(\bar{\alpha} - \sigma_\alpha^2) + \sqrt{2\pi}e^{\frac{(\bar{\alpha}-\sigma_\alpha^2)^2}{2\sigma_\alpha^2}}(\sigma_\alpha^2 + (\bar{\alpha} - \sigma_\alpha^2)^2)\right.$$

$$\left.\times\left[1 + \operatorname{erf}\left(\frac{\bar{\alpha} - \sigma_\alpha^2}{\sqrt{2}\sigma_\alpha}\right)\right]\right\}\left[1 + \operatorname{erf}\left(\frac{\bar{\alpha}}{\sqrt{2}\sigma_\alpha}\right)\right]^{-1}.$$

Using Wolfram Mathematica 12 (with numerical verification), $P_{n|\alpha}$ with arbitrary n can be written in terms of the gamma function Γ and the confluent hypergeometric function of the first kind of $_1F_1$,

$$P_{n|\alpha} = \frac{2^{\frac{n+1}{2}}e^{-\frac{\bar{\alpha}^2}{2\sigma_\alpha^2}}\sigma_\alpha^{n-1}}{\sqrt{2\pi}\,n!}\left\{\sigma_\alpha\Gamma\left(\frac{n+1}{2}\right)_1F_1\left(\frac{n+1}{2},\frac{1}{2},\frac{(\bar{\alpha} - \sigma_\alpha^2)^2}{2\sigma_\alpha^2}\right)\right.$$

$$\left.+ \sqrt{2}(\bar{\alpha} - \sigma_\alpha^2)\Gamma\left(\frac{n+2}{2}\right)_1F_1\left(\frac{n+2}{2},\frac{3}{2},\frac{(\bar{\alpha} - \sigma_\alpha^2)^2}{2\sigma_\alpha^2}\right)\right\} \tag{A10}$$

$$\times\left[1 + \operatorname{erf}\left(\frac{\bar{\alpha}}{\sqrt{2}\sigma_\alpha}\right)\right]^{-1}.$$

Appendix B. Secret Key Length

We consider the efficient BB84 protocol [34] with the basis choice probabilities of $p_X = 0.9$ and $p_Y = 0.1$, in which the X-basis is used for the secret key distillation while the Y-basis is used for the phase error estimation. Since the simultaneous rotation of the bases

around the z-axis does not affect the security, here, for simplicity, we use the notation $\{X, Y\}$ instead of physical $\{X', Y'\}$. The length of the secret key is estimated as follows [42,43],

$$\ell_{\text{sec}}^X = m_1^{X,l}\big[1 - h_2\big(E_1^{\text{ph},X,u}\big)\big] - \text{leak} - 5\log_2\frac{1}{\varepsilon_{\text{pa}}}, \tag{A11}$$

where the first and the last terms represent the privacy amplification step and are determined by $m_1^{X,l}$—the lower bound on the number of bits in the verified key of length ℓ_{ver}^X obtained from signal single-photon pulses, $E_1^{\text{ph},X,u}$—the upper bound on the single-photon phase error rate in the X-basis, and $\varepsilon_{\text{pa}} = 10^{-12}$—the tolerable failure probability for the privacy amplification step. The h_2-function is the standard Shannon binary entropy. The second term in (A11) is the amount of information about the sifted key leaked to Eve during the error correction and verification steps, which can be parametrized as

$$\text{leak} = \ell_{\text{sift}}^X f_{\text{ec}}(\hat{E}_\mu^X) h_2(\hat{E}_\mu^X) + \ell_{\text{hash}}, \tag{A12}$$

where ℓ_{sift}^X is the sifted key length, $\hat{E}_\mu^X$ is the signal quantum bit error rate (QBER), determined during the error correction step, $f_{\text{ec}} \geq 1$ is the error correction code inefficiency, and ℓ_{hash} is the verification hash-tag length. Usually, in the literature, $f_{\text{ec}} \sim 1.2$ is assumed; however, for realistic codes, it can be significantly higher for low QBER. Therefore, we extract the $f_{\text{ec}}(E_\mu)$—dependence of the low-density parity-check (LDPC) codes from Ref. [44] (see the upper-left SEC plot in Figure 3 in [44]).

The finite-key-size effects and statistical fluctuations are taken into account in our analysis. According to the central limit theorem, the binomial distributions of $M_\alpha^X \sim \text{Bi}(N_\alpha^X, Q_\alpha^X)$ and $m_1^X \sim \text{Bi}(\ell_{\text{ver}}^X, Q_1^X/Q_\mu^X)$ can be well approximated by the normal distribution. The upper and lower bounds on Q_α^X and m_1^X are evaluated using the Wald confidence interval [42],

$$Q_\alpha^{X,u(l)} = \hat{Q}_\alpha^X \pm z_{1-\varepsilon}\sqrt{\frac{\hat{Q}_\alpha^X(1 - \hat{Q}_\alpha^X)}{N_\alpha^X}}, \quad \hat{Q}_\alpha^X = \frac{M_\alpha^X}{N_\alpha^X}, \tag{A13}$$

$$m_1^{X,l} = \ell_{\text{ver}}^X \frac{Q_1^{X,l}}{Q_\mu^{X,u}} - z_{1-\varepsilon}\sqrt{\ell_{\text{ver}}^X \frac{Q_1^{X,l}}{Q_\mu^{X,u}}\left(1 - \frac{Q_1^{X,l}}{Q_\mu^{X,u}}\right)}, \quad Q_1^{X,l} = P_{1|\mu}\mathcal{Y}_1^{X,l}, \tag{A14}$$

where N_α^X and M_α^X are the total counts (before sifting) of transmitted and detected pulses of a given intensity, respectively.

It is well known that for the basis-independent source ($\rho_X = \rho_Y$) in the asymptotic limit ($N_\alpha \to \infty$) the phase error rate in the X-basis is equal to the bit error rate in the Y-basis. If $\rho_X \neq \rho_Y$ and the data samples are finite, the phase error bound receives two corrections,

$$E_1^{\text{ph},X,u} = E_1^{Y,u} + \Theta_{\text{coin}} + \Theta_{\text{stat}} = \widetilde{E}_1^{Y,u} + \Theta_{\text{stat}}, \tag{A15}$$

where the basis-dependence correction Θ_{coin} is parametrized in terms of the effective quantum coin imbalance Δ' [40],

$$\Theta_{\text{coin}} = 4\Delta'(1 - \Delta')(1 - 2E_1^{Y,u}) + 4(1 - 2\Delta')\sqrt{\Delta'(1 - \Delta')E_1^{Y,u}(1 - E_1^{Y,u})}, \tag{A16}$$

$$\Delta' = \frac{1 - \sqrt{F(\rho_X, \rho_Y)}}{\mathcal{Y}_1^{X,l} + \mathcal{Y}_1^{Y,l}}, \tag{A17}$$

and Θ_{stat} takes into account different sizes of two random data samples and statistical fluctuations and is determined by the numerical solution of the following equation [43],

$$\sqrt{\frac{m_1^{Y,l} + m_1^{X,l}}{\widetilde{E}_1^{Y,u}(1 - \widetilde{E}_1^{Y,u})m_1^{Y,l}m_1^{X,l}}} \, 2^{-(m_1^{Y,l} + m_1^{X,l})\xi(\Theta_{\text{stat}})} = \varepsilon, \tag{A18}$$

$$\xi(\Theta_{\text{stat}}) = h_2\left(\widetilde{E}_1^{Y,u} + \frac{m_1^{X,l}}{m_1^{Y,l} + m_1^{X,l}}\Theta_{\text{stat}}\right) - \frac{m_1^{Y,l}}{m_1^{Y,l} + m_1^{X,l}}h_2(\widetilde{E}_1^{Y,u})$$
$$- \frac{m_1^{X,l}}{m_1^{Y,l} + m_1^{X,l}}h_2(\widetilde{E}_1^{Y,u} + \Theta_{\text{stat}}). \tag{A19}$$

As pointed out in Ref. [42], in general, one cannot use binomial distribution for QBER since if Eve performs a coherent attack, the errors in different positions in the key cannot be treated as independent events. Therefore, the upper bound on the single-photon bit error rate is estimated differently compared to Ref. [43],

$$E_1^{Y,u} = \frac{\ell_{\text{sift}}^Y \hat{E}_\mu^Y - \overline{m}_0^{Y,l}}{m_1^{Y,l}}, \tag{A20}$$

where the number of bit errors, obtained from the zero-photon pulses due to background events, is distributed as $\overline{m}_0^Y \sim \text{Bi}(N_\mu^Y, p_Y P_{0|\mu}\mathcal{Y}_0^Y/2)$ and lower bounded by

$$\overline{m}_0^{Y,l} = N_\mu^Y p_Y \frac{P_{0|\mu}\mathcal{Y}_0^{Y,l}}{2} - z_{1-\varepsilon}\sqrt{N_\mu^Y p_Y \frac{P_{0|\mu}\mathcal{Y}_0^{Y,l}}{2}\left(1 - p_Y\frac{P_{0|\mu}\mathcal{Y}_0^{Y,l}}{2}\right)}. \tag{A21}$$

Since the Y-basis is used only for parameter estimation, the signal QBER $\hat{E}_\mu^Y$ is computed directly from public disclosure of the sifted keys generated in the Y-basis. All other quantities in the Y-basis are computed the same way as in the X-basis with replacement $\ell_{\text{ver}}^X \to \ell_{\text{sift}}^Y$ in Equation (A14).

One can count 14 statistical confidence bounds in total that are required to compute ℓ_{sec}^X. Therefore, in order to have the estimation (A11) satisfied with the probability not less than $1 - \varepsilon_{\text{decoy}}$, one has to set the failure probability of each bound $\varepsilon = \varepsilon_{\text{decoy}}/14$. We set $\varepsilon_{\text{decoy}} = 10^{-12}$.

For the numerical simulation of $\hat{Q}_\alpha$ and $\hat{E}_\alpha$, we use the simplest theoretical model from Ref. [23],

$$Q_\alpha = 2p_{\text{dc}} + 1 - e^{-t\eta\alpha}, \quad E_\alpha = \frac{p_{\text{dc}} + p_{\text{opt}}(1 - e^{-t\eta\alpha})}{2p_{\text{dc}} + 1 - e^{-t\eta\alpha}}, \tag{A22}$$

with the single-photon detector quantum efficiency of $\eta = 10\%$ and dark count probability of $p_{\text{dc}} = 10^{-6}$, photon transmission probability of $t = 10^{-(\beta L+3)/10}$ determined by Bob's internal loss of $3\,\text{dB}$ and quantum channel loss coefficient $\beta \simeq 0.2\,\text{dB/km}$, and optical misalignment error of $p_{\text{opt}} = 1\%$. For the statistical analysis, we set

$$N_\mu^X = \frac{\ell_{\text{sift}}^X}{p_X Q_\mu}, \quad N_{\nu_i}^X = N_\mu^X \frac{p_{\nu_i}}{p_\mu}, \quad N_\alpha^Y = N_\alpha^X \frac{p_Y}{p_X}, \quad \ell_{\text{sift}}^Y = \ell_{\text{sift}}^X \frac{p_Y^2}{p_X^2}, \tag{A23}$$

where we take the X-basis sifted key block length of $\ell_{\text{sift}}^X = 1.36 \times 10^6$ [44]. We also neglect the error correction and verification failure probabilities and set $\ell_{\text{ver}}^X = \ell_{\text{sift}}^X$.

References

1. 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, 9–12 December 1984; IEEE: New York, NY, USA, 1984; pp. 175–179. [CrossRef]
2. Mayers, D. Quantum key distribution and string oblivious transfer in noisy channels. In Proceedings of the Advances in Cryptology—CRYPTO'96, Santa Barbara, CA, USA, 18–22 August 1996; pp. 343–357. [CrossRef]
3. Koashi, M.; Preskill, J. Secure Quantum Key Distribution with an Uncharacterized Source. *Phys. Rev. Lett.* **2003**, *90*, 057902. [CrossRef]

4.   Lo, H.K.; Chau, H.F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science* **1999**, *283*, 2050–2056. [CrossRef] [PubMed]

5.   Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef] [PubMed]

6.   Koashi, M. Simple security proof of quantum key distribution based on complementarity. *New J. Phys.* **2009**, *11*, 045018. [CrossRef]

7.   Gottesman, D.; Lo, H.K.; Lüttkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.* **2004**, *4*, 325–360. [CrossRef]

8.   Tamaki, K.; Curty, M.; Kato, G.; Lo, H.K.; Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **2014**, *90*, 052314. [CrossRef]

9.   Xu, F.; Wei, K.; Sajeed, S.; Kaiser, S.; Sun, S.; Tang, Z.; Qian, L.; Makarov, V.; Lo, H.K. Experimental quantum key distribution with source flaws. *Phys. Rev. A* **2015**, *92*, 032305. [CrossRef]

10.   Tang, Z.; Wei, K.; Bedroya, O.; Qian, L.; Lo, H.K. Experimental measurement-device-independent quantum key distribution with imperfect sources. *Phys. Rev. A* **2016**, *93*, 042308. [CrossRef]

11.   Mizutani, A.; Curty, M.; Lim, C.C.W.; Imoto, N.; Tamaki, K. Finite-key security analysis of quantum key distribution with imperfect light sources. *New J. Phys.* **2015**, *17*, 093011. [CrossRef]

12.   Mizutani, A.; Kato, G.; Azuma, K.; Curty, M.; Ikuta, R.; Yamamoto, T.; Imoto, N.; Lo, H.K.; Tamaki, K. Quantum key distribution with setting-choice-independently correlated light sources. *npj Quantum Inf.* **2019**, *5*, 8. . [CrossRef]

13.   Pereira, M.; Curty, M.; Tamaki, K. Quantum key distribution with flawed and leaky sources. *npj Quantum Inf.* **2019**, *5*, 62. [CrossRef]

14.   Pereira, M.; Kato, G.; Mizutani, A.; Curty, M.; Tamaki, K. Quantum key distribution with correlated sources. *Sci. Adv.* **2020**, *6*, eaaz4487. [CrossRef]

15.   Currás-Lorenzo, G.; Navarrete, A.; Pereira, M.; Tamaki, K. Finite-key analysis of loss-tolerant quantum key distribution based on random sampling theory. *Phys. Rev. A* **2021**, *104*, 012406. [CrossRef]

16.   Pereira, M.; Currás-Lorenzo, G.; Navarrete, A.; Mizutani, A.; Kato, G.; Curty, M.; Tamaki, K. Modified BB84 quantum key distribution protocol robust to source imperfections. *Phys. Rev. Res.* **2023**, *5*, 023065. [CrossRef]

17.   Currás-Lorenzo, G.; Pereira, M.; Kato, G.; Curty, M.; Tamaki, K. A security framework for quantum key distribution implementations. *arXiv* **2023**, arXiv:2305.05930.

18.   Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330–1333. [CrossRef]

19.   Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. [CrossRef]

20.   Hwang, W.Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]

21.   Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]

22.   Wang, X.B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]

23.   Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]

24.   Trushechkin, A.; Kiktenko, E.; Kronberg, D.; Fedorov, A. Security of the decoy state method for quantum key distribution. *Physics-Uspekhi* **2021**, *64*, 88. [CrossRef]

25.   Lucamarini, M.; Choi, I.; Ward, M.; Dynes, J.; Yuan, Z.; Shields, A. Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution. *Phys. Rev. X* **2015**, *5*, 031030. [CrossRef]

26.   Tamaki, K.; Curty, M.; Lucamarini, M. Decoy-state quantum key distribution with a leaky source. *New. J. Phys.* **2016**, *18*, 065008. [CrossRef]

27.   Wang, W.; Tamaki, K.; Curty, M. Finite-key security analysis for quantum key distribution with leaky sources. *New. J. Phys.* **2018**, *20*, 083027. [CrossRef]

28.   Molotkov, S. Trojan horse attacks, decoy state method, and side channels of information leakage in quantum cryptography. *J. Exp. Theor. Phys.* **2020**, *130*, 809–832. [CrossRef]

29.   Molotkov, S. Side channels of information leakage in quantum cryptography: Nonstrictly single-photon states, different quantum efficiencies of detectors, and finite transmitted sequences. *J. Exp. Theor. Phys.* **2021**, *133*, 272–304. [CrossRef]

30.   Wang, X.B.; Peng, C.Z.; Zhang, J.; Yang, L.; Pan, J.W. General theory of decoy-state quantum cryptography with source errors. *Phys. Rev. A* **2008**, *77*, 042311. [CrossRef]

31.   Wang, X.B.; Yang, L.; Peng, C.Z.; Pan, J.W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New. J. Phys.* **2009**, *11*, 075006. [CrossRef]

32.   Foletto, G.; Picciariello, F.; Agnesi, C.; Villoresi, P.; Vallone, G. Security bounds for decoy-state quantum key distribution with arbitrary photon-number statistics. *Phys. Rev. A* **2022**, *105*, 012603. [CrossRef]

33.   Wang, W.; Wang, R.; Hu, C.; Zapatero, V.; Qian, L.; Qi, B.; Curty, M.; Lo, H.K. Fully Passive Quantum Key Distribution. *Phys. Rev. Lett.* **2023**, *130*, 220801. [CrossRef] [PubMed]

34. Lo, H.K.; Chau, H.; Ardehali, M. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. *J. Cryptol.* **2005**, *18*, 133–165. [CrossRef]
35. Huang, A.; Mizutani, A.; Lo, H.K.; Makarov, V.; Tamaki, K. Characterization of State-Preparation Uncertainty in Quantum Key Distribution. *Phys. Rev. Appl.* **2023**, *19*, 014048. [CrossRef]
36. Huang, A.; Sun, S.H.; Liu, Z.; Makarov, V. Quantum key distribution with distinguishable decoy states. *Phys. Rev. A* **2018**, *98*, 012330. [CrossRef]
37. Duplinskiy, A.; Ustimchik, V.; Kanapin, A.; Kurochkin, V.; Kurochkin, Y. Low loss QKD optical scheme for fast polarization encoding. *Opt. Express* **2017**, *25*, 28886–28897. [CrossRef]
38. Zapatero, V.; Wang, W.; Curty, M. A fully passive transmitter for decoy-state quantum key distribution. *Quantum Sci. Technol.* **2023**, *8*, 025014. [CrossRef]
39. Tamaki, K.; Koashi, M.; Imoto, N. Unconditionally Secure Key Distribution Based on Two Nonorthogonal States. *Phys. Rev. Lett.* **2003**, *90*, 167904. [CrossRef]
40. Lo, H.K.; Preskill, J. Security of Quantum Key Distribution Using Weak Coherent States with Nonrandom Phases. *Quantum Info. Comput.* **2007**, *7*, 431–458. [CrossRef]
41. Jozsa, R. Fidelity for Mixed Quantum States. *J. Mod. Opt.* **1994**, *41*, 2315–2323. [CrossRef]
42. Trushechkin, A.; Kiktenko, E.; Fedorov, A. Practical issues in decoy-state quantum key distribution based on the central limit theorem. *Phys. Rev. A* **2017**, *96*, 022316. [CrossRef]
43. Zhang, Z.; Zhao, Q.; Razavi, M.; Ma, X. Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Phys. Rev. A* **2017**, *95*, 012333. [CrossRef]
44. Borisov, N.; Petrov, I.; Tayduganov, A. Asymmetric Adaptive LDPC-Based Information Reconciliation for Industrial Quantum Key Distribution. *Entropy* **2023**, *25*, 31. [CrossRef] [PubMed]