New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

PAPER • OPEN ACCESS

Finite-key security analysis of quantum key distribution with imperfect light sources

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

CrossMark

OPEN ACCESS

RECEIVED
1 May 2015

REVISED
20 July 2015

ACCEPTED FOR PUBLICATION
6 August 2015

PUBLISHED
9 September 2015

PAPER

Finite-key security analysis of quantum key distribution with imperfect light sources

Akihiro Mizutani[1], **Marcos Curty**[2], **Charles Ci Wen Lim**[3,4], **Nobuyuki Imoto**[1] **and Kiyoshi Tamaki**[5]

[1] Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan
[2] EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
[3] Group of Applied Physics, University of Geneva, Geneva CH-1211, Switzerland
[4] Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831-6418, USA
[5] NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato-Wakamiya Atsugi-Shi, 243-0198, Japan

E-mail: mizutani@qi.mp.es.osaka-u.ac.jp

Keywords: quantum key distribution, security analysis, quantum optics

Abstract

In recent years, the gap between theory and practice in quantum key distribution (QKD) has been significantly narrowed, particularly for QKD systems with arbitrarily flawed optical receivers. The status for QKD systems with imperfect light sources is however less satisfactory, in the sense that the resulting secure key rates are often overly dependent on the quality of state preparation. This is especially the case when the channel loss is high. Very recently, to overcome this limitation, Tamaki *et al* proposed a QKD protocol based on the so-called 'rejected data analysis', and showed that its security—in the limit of infinitely long keys—is almost independent of any encoding flaw in the qubit space, being this protocol compatible with the decoy state method. Here, as a step towards practical QKD, we show that a similar conclusion is reached in the finite-key regime, even when the intensity of the light source is unstable. More concretely, we derive security bounds for a wide class of realistic light sources and show that the bounds are also efficient in the presence of high channel loss. Our results strongly suggest the feasibility of long distance provably secure communication with imperfect light sources.

1. Introduction

The gist of quantum key distribution (QKD) [1–3] is that it allows two remote parties, Alice and Bob, to establish common secret keys in the presence of an adversary, Eve, who may have unlimited computing resources and technological advances. Today, three decades after its introduction, QKD has made enormous progress in both theory and practice, and is arguably on the verge of global commercialization. Having said that, however, there are still some issues, both theoretical and experimental, that need to be resolved before we can reach that level. Amongst those, the most pressing one is the mismatch between device models used in security proofs and actual devices used in QKD systems. In particular, such implementation loopholes can lead to side-channel attacks that break the security of QKD. Notably, it has been repeatedly demonstrated that the behaviour of single-photon detectors employed in QKD systems can be externally controlled, simply by exploiting their physics [4]. In this case, it is easy to verify that security cannot be achieved, since the measured data are not representative of the quantum channel [5]. Undoubtedly, such hacking demonstrations raise not only the importance of proper calibration of QKD systems, but also the importance in developing security proof techniques that can tackle modeling discrepancies. Indeed, in the past few years, much attention has been devoted towards the development of such proof techniques and side-channel countermeasures, particularly in the areas of security of finite-length keys [6–10] and detector side-channel attacks [11, 14, 15, 12, 13].

Amongst these theoretical results, only a few considered the issue of state preparation flaws—despite that it is a commonly faced experimental problem. More concretely, typical light sources used in QKD systems are not true single-photon sources and practical optical modulators employed to encode the light pulses are inherently limited in precision. The former can be resolved by using the decoy-state method [16–18], which allows QKD systems based on practical light sources to achieve the security performance of single-photon QKD. The latter, however, does not have an adequate solution. In particular, it has been firstly shown by Gottesman *et al* [19] that such inaccuracies in encoding can lead to very pessimistic secret key rates in the presence of high quantum channel loss. Also, other works show similar results [20]. This strong dependency on channel loss is primarily due to the fact that state preparation flaws can be seen as a form of basis information leakage, which gives Eve some advantage in formulating basis-dependent attacks. Crucially, as shown in [19, 20], Eve's advantage can be significantly enhanced by exploiting channel losses. Consequently, this heavily penalizes the secret key rate whenever the channel loss is substantial.

Very recently, a loss-tolerant QKD protocol [21] has been proposed by Tamaki *et al* as a means to overcome typical encoding flaws in QKD systems. More specifically, as briefly mentioned earlier, here we are considering encoding flaws due to imprecise alignment of optical modulators. For example, if the quantum states are encoded into the polarization degree-of-freedom of photons, an encoding flaw could be due to a misalignment in the wave-plate used to set the desired polarization. The protocol is similar to the Bennett–Brassard 1984 (BB84) QKD scheme [22], but instead of considering all the four BB84 states, it uses only three of them. Interestingly, by considering statistics beyond those of the BB84 protocol, the resulting secret key rate is the same as the one of BB84's [23–27]. More importantly, the secret key rate has the very nice property in that it is almost independent of encoding flaws. These results imply that the usual stringent demand on precise state preparation can be considerably relaxed and one only needs to know the prepared states. Additionally, it is useful to mention that most current BB84 QKD systems can easily switch to the loss-tolerant QKD protocol without much hardware modifications.

In anticipation that the loss-tolerant QKD protocol will be widely implemented in the near future, we extend the security analysis in [21] to the finite-key regime, i.e., we derive explicit bounds on the extractable secret key length (in [28], the authors have implemented the loss-tolerant protocol experimentally with careful verification of the qubit assumption used in the protocol. This paper also includes some finite-key analysis of the protocol. Unfortunately, however, its phase error rate estimation seems to be valid only against collective attacks). Furthermore, our bounds can be applied to a wide range of imperfect light sources —including typical cases whereby the intensity of the laser is fluctuating between a certain range[6].

Also, the security bounds are obtained within the so-called universal-composable framework [30], and thus secret keys generated using these bounds can be applied to other cryptographic tasks like the one-time-pad. In order to investigate the feasibility of our results, we consider a QKD system model that borrows parameters from recent fibre-based QKD experiments. With this realistic model, our numerical simulations show that provably-secure keys can be distributed up to a fibre length of about 120 km, even when only 10^{11} signals are sent by Alice to Bob.

This paper is organized as follows. In section 2, we describe some assumptions that we made in our security analysis and after that we introduce our protocol. In section 3, we give the security definition of the protocol and provide the formulation of the extractable secret key length. In section 4, we present the results of the parameter estimation using the decoy-state method for two different cases: an exact intensity control case and an intensity-fluctuation case. Then, in section 5, we simulate the key generation rate for both scenarios. Finally, section 6 concludes the paper with a summary. The paper includes as well some appendixes with additional calculations.

2. Assumptions and description of the protocol

2.1. Assumptions on Alice and Bob's devices

Prior to stating the actual protocol, we first describe the assumptions on the user's devices.

We consider that Alice's transmitter contains a laser source, an amplitude modulator and a phase modulator. See figure 1. The laser is single-mode and emits signals with a Poissonian photon number distribution. Also, we assume that Alice encodes the bit and the basis information in the relative phase θ_A between a signal and a reference pulse, whose joint phase is perfectly randomized[7]. Let us emphasize, however, that the security proof that we provide in this paper applies as well to other coding schemes like, for instance, the polarization or the time-bin coding schemes. Next we present the two types of imperfections that we consider for Alice's device.

[6] In the asymptotic limit of an infinitely long key, the problem of intensity fluctuations in decoy-state QKD has been considered in [29].

[7] Note that the recent work [31] shows that discrete phase randomization is sufficient for the BB84 protocol.

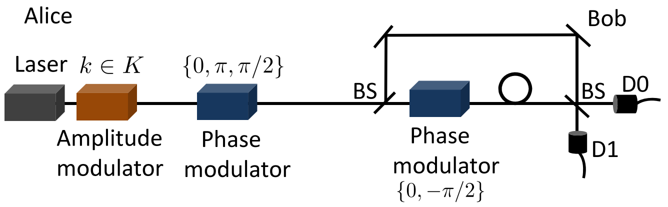

Figure 1. In each trial, Alice's laser emits two consecutive coherent pulses representing the signal and the reference pulse. For this, she first uses an amplitude modulator to select the pulses' intensity $k \in K$. After that, she applies a phase shift $\{0, \pi, \pi/2\}$ to the signal pulse. On reception, Bob splits the received pulses into two beams and then applies a phase shift $\{0, -\pi/2\}$ to one of them. Also, he applies a one-pulse delay to one of the arms of the interferometer and then recombine the pulses at a 50:50 beamsplitter (BS). A 'click' in detector D0 (D1) provides Bob the key bit $y' = 0$ ($y' = 1$).

(1) *Intensity fluctuations.*

The fluctuation of the intensity of the emitted coherent light is typically due to the laser source and imperfections in the amplitude modulator. Here we shall consider that Alice does not have a full description of the probability density function of the fluctuations, but she only knows their range[8]. That is, she knows that the intensity k of the emitted coherent light lies in an interval $k \in [k^-, k^+]$ except with error probability $\epsilon_{\rm inten}$, where $k^{+(-)}$ is the upper (lower) intensity. Moreover, we assume that the intensities of the coherent pulses are not independent to each other, that is, they can be correlated in an arbitrary manner as long as they lie in the interval. For simplicity, we shall assume that $\epsilon_{\rm inten} = 0$. If $\epsilon_{\rm inten} > 0$ this error probability can be directly taken into account through the security parameter $\epsilon_{\rm sec}$ whose definition is referred to equation (40). The intensities of the signal and reference pulses are $k^{\rm sig} := kV$ and $k^{\rm ref} := k(1 - V)$ respectively, with $0 < V < 1$.

In section 4. A we study the case where $k = k^- = k^+$, i.e., there are no intensity fluctuations. After that, in section 4. B, we evaluate the typical scenario where $k^+ > k^-$.

(2) *Imperfect encoding of the bit and basis information.*

In our protocol, Alice chooses the relative phase $\theta_{\rm A}$ at random from $\{0, \pi/2, \pi\}$ to encode the bit and basis information. The phase $\theta_{\rm A} \in \{0, \pi\}$ corresponds to the Z basis states which are selected with equal probability, and $\theta_{\rm A} = \pi/2$ denotes the X basis state. Alice assigns a bit value $y = 0$ to $\theta_{\rm A} \in \{0, \pi/2\}$ and a bit value $y = 1$ to $\theta_{\rm A} = \pi$.

Due to the misalignment of the optical system, however, the actual relative phase prepared by Alice may deviate from the desired angle $\theta_{\rm A}$ by a factor $\Delta\theta_{\rm A}$. Hence, we have that the actual state Alice sends to Bob can be typically described as

$$\int_0^{2\pi} p\left(\Delta\theta_{\rm A}\right) P\left[\left|\sqrt{k^{\rm ref}}\,{\rm e}^{{\rm i}\chi}\right\rangle_{\rm r}\left|\sqrt{k^{\rm sig}}\,{\rm e}^{{\rm i}\left(\chi+\theta_{\rm A}+\Delta\theta_{\rm A}\right)}\right\rangle_{\rm s}\right]{\rm d}\Delta\theta_{\rm A}. \tag{1}$$

Here, we define $P[\,\cdot\,] = |\,\cdot\,\rangle\langle\,\cdot\,|$, the parameter $\chi \in [0, 2\pi)$ is a random phase, the state $|\alpha\rangle_{\rm s(r)}$ is the coherent state of the signal (reference) pulse, and $p(\Delta\theta_{\rm A})$ is the probability distribution of $\Delta\theta_{\rm A}$.

Alice does not need to know the origin of the encoding errors $\Delta\theta_{\rm A}$, but we assume that she knows $p(\Delta\theta_{\rm A})$. Also, we assume that $p(\Delta\theta_{\rm A})$ is independently and identically distributed for each run of the protocol. Moreover, we consider that there are no side-channels in Alice's device.

Assumptions on Bob's apparatus

We consider that the detection efficiency of Bob's detectors is independent of his measurement basis choice. A phase value $\theta_{\rm B} = 0$ ($\theta_{\rm B} = -\pi/2$) corresponds to a device parameter to choose the Z (X) basis for the measurement. Also, like in the case of Alice, we consider that Bob uses an imperfect phase modulator that shifts the phase of the incoming signals by $\theta_{\rm B} + \Delta\theta_{\rm B}$, where $\Delta\theta_{\rm B}$ is the modulation error. Note, however, that this last assumption is not needed in the security proof; we use it only for simulating the resulting secret key rate. Furthermore, we assume that there are no side-channels in Bob's device.

2.2. Protocol description

We study a three-state protocol that uses one signal and two decoy settings. Also, we consider that the protocol employs an asymmetric coding, i.e., the Z and the X basis are chosen with probabilities p_z and $p_x = 1 - p_z$, respectively. The secret key is extracted only from those events where both Alice and Bob select the Z basis and the signal setting. In addition, we assume that Alice and Bob do not implement a random sampling procedure to estimate the bit error rate, but they perform error correction for a pre-established fixed value of it. The error verification step of the protocol (see step 5 below) informs them about whether or not the actual residual bit error rate exceeds the considered value.

[8] Note that in those scenarios where Alice knows the exact probability distribution of the fluctuations then the conventional decoy-state method can be directly applied.

The protocol runs as follows.

Actual protocol

First, Alice and Bob decide a security parameter ϵ_{sec} whose definition is referred to equation (40). Then, they repeat the first three steps of the protocol for $i = 1, \ldots, N$ until the conditions in the sifting step are met.

(1) *Preparation*

For each i, Alice randomly chooses the intensity $k \in K = \{k_{\text{s}}, k_{\text{d1}}, k_{\text{d2}}\}$ with probability $p_{k_{\text{s}}}$, $p_{k_{\text{d1}}}$ and $p_{k_{\text{d2}}} = 1 - p_{k_{\text{s}}} - p_{k_{\text{d1}}}$, respectively. The intervals $[k^-, k^+]$ where the different intensities lie have to satisfy $k_{\text{d1}}^- > k_{\text{d2}}^+$ and $k_{\text{s}}^- > k_{\text{d1}}^+ + k_{\text{d2}}^-$. Then, Alice randomly selects the basis $a \in \{Z, X\}$ with probabilities p_z and p_x, respectively. Next, she chooses at random the signal phase $\theta_{\text{A}} \in \{0, \pi\}$ when she selects the Z basis, and she chooses $\theta_{\text{A}} = \pi/2$ when she selects the X basis. Finally, she generates the signal and reference pulses following these specifications and sends them to Bob via the quantum channel.

(2) *Measurement*

Bob measures the incoming signal and reference pulses using the measurement basis $b \in \{Z, X\}$,which he randomly selects with probabilities p_z and p_x, respectively. The outcome is recorded in $d \in \{0, 1, \perp, \varnothing\}$, where $\perp$ and $\varnothing$ represent the double click event and the no click event, respectively. If $d = \perp$, Bob assigns a random bit to it[9]. As a result, he obtains $y' = \{0, 1, \varnothing\}$.

(3) *Sifting*

Alice and Bob announce their bases and intensity choices over an authenticated public channel and identify the following sets: $Z_k := \{i | a = b = Z \wedge \text{Intensity} = k \wedge y' \neq \varnothing\}$, $X_k^j := \{i | a = b = X \wedge \text{Intensity} = k \wedge y' = j\}$, $Z^{0(1)}X_k^j := \{i | a = Z \wedge b = X \wedge \text{Intensity} = k \wedge y = 0\ (1) \wedge y' = j\}$ and $XZ_k^j := \{i | a = X \wedge b = Z \wedge \text{Intensity} = k \wedge y' = j\}$ with $j \in \{0, 1\}$ and $k \in K$. Then, they check if the following conditions are met: $|Z_k| \geqslant N_{Z_k}$, $|X_k^j| \geqslant N_{X_k^j}$, $|Z^{0(1)}X_k^j| \geqslant N_{Z^{0(1)}X_k^j}$ and $|XZ_k^j| \geqslant N_{XZ_k^j}$ for all $j \in \{0, 1\}$, all $k \in K$, and for certain pre-established values N_{Z_k}, $N_{X_k^j}$, $N_{Z^{0(1)}X_k^j}$ and $N_{XZ_k^j}$,where $| * |$ represents the length of the set $*$.

We denote by N the number of pairs of coherent states (i.e., signal and reference pulses) sent by Alice until these conditions are fulfiled. We denote Alice and Bob's sifted keys as $(Z_{\text{A}}, Z_{\text{B}})$; their size is $|Z_{\text{A}}| = |Z_{\text{B}}| = |Z_{k_{\text{s}}}|$.

(4) *Parameter estimation*

They estimate the number of events $m_{0(1)}$, where Alice emitted the vacuum (the single-photon) state within the set $Z_{k_{\text{s}}}$. Their expression is given by equations (12) and (18) for the scenario without intensity fluctuations, and by equations (23) and (28) for the case with intensity fluctsuations. Also, Alice and Bob estimate N_{ph}, i.e., the number of the so-called phase errors in the single-photon emissions within the set $Z_{k_{\text{s}}}$ (see equation (36)). They check if the phase error rate $e_{\text{ph}} := N_{\text{ph}}/m_1$ is lower than a predetermined threshold value $\overline{e_{\text{ph}}}$, which corresponds to the phase error rate associated with a zero secret key rate (see equation (2)). If $e_{\text{ph}} \geqslant \overline{e_{\text{ph}}}$ they abort the protocol; otherwise they proceed to step 5.

(5) *Postprocessing*

Alice and Bob perform error correction over an authenticated public channel for $(Z_{\text{A}}, Z_{\text{B}})$. This step consumes at most λ_{EC} bits. Finally, they implement an error verification step and, after that, they perform privacy amplification using a hash function that extracts a secret key pair $(S_{\text{A}}, S_{\text{B}})$, where $|S_{\text{A}}| = |S_{\text{B}}| = \ell$ bits.

3. Security bounds

The security of a QKD protocol is characterized by its *correctness* and *secrecy*. That is, following the universal composable security framework [30], the protocol is called ϵ_{sec}-secure if it is both ϵ_{c}-correct and ϵ_{s}-secret, where $\epsilon_{\text{sec}} = \epsilon_{\text{c}} + \epsilon_{\text{s}}$. Here, the correctness criterion is met whenever the output keys, S_{A} and S_{B}, are identical. More generally, for some small error ϵ_{c} in the correctness, we say that the protocol is ϵ_{c}-correct if $\Pr[S_{\text{A}} \neq S_{\text{B}}] \leqslant \epsilon_{\text{c}}$ is met. For the secrecy criterion, it is met whenever the joint classical-quantum state describing Alice's output key and Eve's quantum system is of the following form, $U_{\text{A}} \otimes \rho_{\text{E}}$, where U_{A} is the uniform distribution over all bit strings, and ρ_{E} is an arbitrary quantum state held by Eve. Likewise, for some small error ϵ_{s}, we say the protocol is ϵ_{s}-secret if

$$\frac{1}{2} \parallel \rho_{\text{S}_{\text{A}}\text{E}} - U_{\text{A}} \otimes \rho_{\text{E}} \parallel_1 \leqslant \epsilon_{\text{s}},$$

where $\rho_{\text{S}_{\text{A}}\text{E}}$ is the joint state shared by Alice and Eve. Note that $|| \cdot ||_1$ is the trace norm defined as $|| \cdot ||_1 = \text{Tr}\sqrt{\cdot^{\dagger}\cdot}$. Using these security definitions, it can be shown (see appendix A for details) that a lower bound on the secret key length for the protocol described above

$$\ell \geqslant \left\lfloor m_0^{\text{L}} + m_1^{\text{L}}\left[1 - h\left(e_{\text{ph}}^{\text{U}}\right)\right] - \log_2\frac{2}{\epsilon_{\text{s}}^2 - \eta} - \lambda_{\text{EC}} - \log_2\frac{2}{\epsilon_{\text{c}}}\right\rfloor, \tag{2}$$

[9] Note that this random assignment is not mandatory, and Bob can always choose a particular bit value, say 0, for $d = \perp$ as this preserves the basis-independence detection efficiency condition.

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function, $m_{0(1)}^{\mathrm{L}}$ is a lower bound on $m_{0(1)}$, $e_{\mathrm{ph}}^{\mathrm{U}} := N_{\mathrm{ph}}^{\mathrm{U}}/m_1^{\mathrm{L}}$ is an upper bound on the phase error rate, and η is the sum of the failure probabilities when estimating m_0 and e_{ph}. This last parameter is upper bounded by $\eta \leqslant 1 - E_{Z,0}E_{Z,1}E_{\mathrm{ph}}$, where $E_{Z,0}$, $E_{Z,1}$ and E_{ph} are the failure probabilities associated to the estimation of m_0^{L}, m_1^{L} and to the upper bound on the number of the phase errors $N_{\mathrm{ph}}^{\mathrm{U}}$, respectively.

4. Parameter estimation

In this section, we briefly describe the estimation procedure to obtain m_0^{L} and m_1^{L}. Also, we provide an expression for $N_{\mathrm{ph}}^{\mathrm{U}}$. The detailed calculations are included in appendix D.

As mentioned in section 2.2, we assume that the phase of each pulse generated by the laser is perfectly randomized. This means, in particular, that we can regard the signals sent by Alice as a classical mixture of Fock states, each of them representing the total number of photons contained both in the signal and in the reference pulse. That is, the probability that Alice emits a pulse with n photons conditioned on the fact that she selects the intensity setting $k \in K$ is written as

$$p(n|k) = \mathrm{e}^{-k}\frac{k^n}{n!}. \tag{3}$$

Also, from the property of the decoy state method we have that the total number of detection events when both Alice and Bob use the Z basis is given by

$$|Z_{\mathrm{tot}}| := \sum_{k\in K}\left|Z_k\right| = \sum_{n=0}^{\infty} S_{Z,n}, \tag{4}$$

where $S_{Z,n}$ represents the number of detection events when Alice and Bob used the Z basis and Alice emitted an n-photon state.

4.1. Estimation of the number of vacuum and single-photon contributions for the exact intensity control case

We consider first the scenario without intensity fluctuations in the source, i.e., when $k = k^- = k^+$.

Owing to the use of decoy-states [16–18], it can be shown that Eve cannot obtain any useful information about Alice's intensity choice if she observes an n-photon state in the quantum channel. Therefore, it can be demonstrated that the *actual* protocol, where Alice chooses the intensity of each signal before she actually sends it to Bob, is equivalent to a *counterfactual* protocol described as follows. First, Alice prepares and sends n-photon states to Bob. Then, Bob measures all the signals received from Alice. Afterwards, Alice decides the intensity setting for each signal. Due to this equivalence between the actual and the counterfactual protocols, we have that the number of detection events $|Z_k|$ for setting $k \in K$ within $|Z_{\mathrm{tot}}|$ has the form

$$|Z_k| = \langle Z_k\rangle + \delta_k, \tag{5}$$

except with certain error probability that will be introduced later on, and where $\langle Z_k\rangle$ denotes the mean value of $|Z_k|$ given by

$$\langle Z_k\rangle = \sum_{n=0}^{\infty} p(k|n)S_{Z,n}. \tag{6}$$

Here, $p(k|n)$ is the conditional probability of choosing the intensity k given that Alice prepared a n-photon state. The parameter δ_k that appears in equation (5) denotes the deviation between the experimentally obtained quantity $|Z_k|$ and its expected value. The convergence of δ_k is discussed in appendix B.

4.1.1. Estimation of the number of vacuum contributions

At first, we calculate a lower bound on m_0, the number of events in $Z_{k_{\mathrm{s}}}$ that originate from a vacuum state sent by Alice. We define the mean value of m_0 as $\mu_0 = p(k_{\mathrm{s}}|0)S_{Z,0}$. Now, by applying *lemma 1* from appendix B we obtain that

$$m_0 \geqslant \mu_0 - \Delta_{Z,0}, \tag{7}$$

except with certain error probability $\epsilon_{Z,0}$, where the deviation $\Delta_{Z,0}$ is given by $\Delta_{Z,0} = g_{\mathrm{C}}(\mu_0, \epsilon_{Z,0})$ with $g_{\mathrm{C}}(x, y) = \sqrt{2x\ln 1/y}$. So far, the lower bound on m_0 depends on the unknown mean value μ_0 which cannot be directly observed in the experiment. According to the definition of μ_0, however, this problem can be solved by estimating a lower bound on $S_{Z,0}$. For this, we use a result from [8]. In particular, we have that

$$S_{Z,0} \geqslant \frac{p(0)}{k_{\mathrm{d1}} - k_{\mathrm{d2}}} \left(\frac{k_{\mathrm{d1}} \mathrm{e}^{k_{\mathrm{d2}}}}{p_{k_{\mathrm{d2}}}} \left\langle Z_{k_{\mathrm{d2}}} \right\rangle - \frac{k_{\mathrm{d2}} \mathrm{e}^{k_{\mathrm{d1}}}}{p_{k_{\mathrm{d1}}}} \left\langle Z_{k_{\mathrm{d1}}} \right\rangle \right) =: S_{Z,0}^{\mathrm{L}}, \tag{8}$$

where $p(0) = \sum_{k \in K} p_k \ p(0|k)$. To estimate the mean values $\langle Z_{k_{\mathrm{d1}}} \rangle$ and $\langle Z_{k_{\mathrm{d2}}} \rangle$, we can employ either *lemmas 2* or *3* introduced in appendix B, such that the fluctuation is minimized. In so doing, we obtain a lower bound on $\langle Z_{k_{\mathrm{d2}}} \rangle$ together with an upper bound on $\langle Z_{k_{\mathrm{d1}}} \rangle$ given by

$$\left\langle Z_{k_{\mathrm{d2}}}^- \right\rangle := |Z_{k_{\mathrm{d2}}}| - \min \left\{ g_{\mathrm{M}} \left(\left| Z_{k\mathrm{d2}} \right|, \left(\epsilon_{Z,0}^{k_{\mathrm{d2}}} \right)^{3/2} \right), g_{\mathrm{H}} \left(\left| Z_{\mathrm{tot}} \right|, \epsilon_{Z,0}^{k_{\mathrm{d2}}} \right) \right\}, \tag{9}$$

$$\left\langle Z_{k_{\mathrm{d1}}}^+ \right\rangle := \left| Z_{k_{\mathrm{d1}}} \right| + \min \left\{ g_{\mathrm{M}} \left(\left| Z_{k\mathrm{d1}} \right|, \left(\epsilon_{Z,0}^{k_{\mathrm{d1}}} \right)^4 / 16 \right), g_{\mathrm{H}} \left(\left| Z_{\mathrm{tot}} \right|, \epsilon_{Z,0}^{k_{\mathrm{d1}}} \right) \right\}, \tag{10}$$

where $g_{\mathrm{M}}(x, y) = \sqrt{2x \ln 1/y}$ and $g_{\mathrm{H}}(x, y) = \sqrt{x/2 \ln 1/y}$. The failure probability associated with the estimation of $\langle Z_k \rangle$, with $k \in \{k_{\mathrm{d1}}, k_{\mathrm{d2}}\}$, is either given by $\varepsilon_{Z,0}^k = \epsilon_{Z,0}^k$ or by $\varepsilon_{Z,0}^k = \epsilon_{Z,0}^k + \epsilon_{\mathrm{H},Z,0}^k$, depending on which *lemmas* (*2* or *3*) we use. As a result we find that

$$\mu_0 \geqslant p\left(k_{\mathrm{s}} \middle| 0\right) S_{Z,0}^{\mathrm{L}} \geqslant \frac{p_{k_{\mathrm{s}}} \mathrm{e}^{-k_{\mathrm{s}}}}{k_{\mathrm{d1}} - k_{\mathrm{d2}}} \left(\frac{k_{\mathrm{d1}} \mathrm{e}^{k_{\mathrm{d2}}}}{p_{k_{\mathrm{d2}}}} \left\langle Z_{k_{\mathrm{d2}}}^- \right\rangle - \frac{k_{\mathrm{d2}} \mathrm{e}^{k_{\mathrm{d1}}}}{p_{k_{\mathrm{d1}}}} \left\langle Z_{k_{\mathrm{d1}}}^+ \right\rangle \right) =: \mu_0^{\mathrm{L}}, \tag{11}$$

which only depends on known parameters. Note that in equation (11) we have used the fact that $p(k_{\mathrm{s}}|0) = p_{k_{\mathrm{s}}} p(0|k_{\mathrm{s}}) / p(0) = p_{k_{\mathrm{s}}} \mathrm{e}^{-k_{\mathrm{s}}} / p(0)$ in combination with equation (8). We finally obtain, therefore, that

$$m_0 \geqslant \mu_0^{\mathrm{L}} - \Delta_{Z,0} =: m_0^{\mathrm{L}}, \tag{12}$$

except with error probability $\varepsilon_{Z,0} = \epsilon_{Z,0} + \varepsilon_{Z,0}^{k_{\mathrm{d1}}} + \varepsilon_{Z,0}^{k_{\mathrm{d2}}}$.

4.1.2. Estimation of the number of single-photon contributions

Here, we calculate a lower bound on the number of single-photon pulses sent by Alice that contribute to $Z_{k_{\mathrm{s}}}$. For this, we use a similar technique to the one described in the previous section. In particular, let μ_1 be the mean value of m_1, which is given by $\mu_1 = p(k_{\mathrm{s}}|1) S_{Z,1}$. Then we have that

$$m_1 \geqslant \mu_1 - \Delta_{Z,1}, \tag{13}$$

except with error probability $\epsilon_{Z,1}$, where $\Delta_{Z,1} = g_{\mathrm{C}}(\mu_1, \epsilon_{Z,1})$. From [8], we have that

$$\begin{aligned} S_{Z,1} \geqslant & \frac{p(1) k_{\mathrm{s}}}{\left(k_{\mathrm{d1}} - k_{\mathrm{d2}}\right)\left(k_{\mathrm{s}} - k_{\mathrm{d1}} - k_{\mathrm{d2}}\right)} \left[\frac{\mathrm{e}^{k_{\mathrm{d1}}}}{p_{k_{\mathrm{d1}}}} \left\langle Z_{k_{\mathrm{d1}}} \right\rangle - \frac{\mathrm{e}^{k_{\mathrm{d2}}}}{p_{k_{\mathrm{d2}}}} \left\langle Z_{k_{\mathrm{d2}}} \right\rangle \right. \\ & \left. + \frac{k_{\mathrm{d1}}^2 - k_{\mathrm{d2}}^2}{k_{\mathrm{s}}^2} \left(\frac{S_{Z,0}^{\mathrm{L}}}{p(0)} - \frac{\mathrm{e}^{k_{\mathrm{s}}} \left\langle Z_{k_{\mathrm{s}}} \right\rangle}{p_{k_{\mathrm{s}}}} \right) \right] =: S_{Z,1}^{\mathrm{L}}, \end{aligned} \tag{14}$$

where $p(1) = \sum_{k \in K} p_k \ p(1|k)$. As before, by using *lemmas* 2 and 3 from appendix B we obtain a lower bound on $\langle Z_{k_{\mathrm{d1}}} \rangle$, and an upper bound on $\langle Z_{k_{\mathrm{d2}}} \rangle$ and $\langle Z_{k_{\mathrm{s}}} \rangle$. They are given by

$$\langle Z_{k_{\mathrm{d1}}}^- \rangle := \left| Z_{k_{\mathrm{d1}}} \right| - \min \left\{ g_{\mathrm{M}} \left(\left| Z_{k\mathrm{d1}} \right|, \left(\epsilon_{Z,1}^{k_{\mathrm{d1}}} \right)^{3/2} \right), g_{\mathrm{H}} \left(\left| Z_{\mathrm{tot}} \right|, \epsilon_{Z,1}^{k_{\mathrm{d1}}} \right) \right\}, \tag{15}$$

$$\langle Z_k^+ \rangle := \left| Z_k \right| + \min \left\{ g_{\mathrm{M}} \left(\left| Z_k \right|, \left(\epsilon_{Z,1}^k \right)^4 / 16 \right), g_{\mathrm{H}} \left(\left| Z_{\mathrm{tot}} \right|, \epsilon_{Z,1}^k \right) \right\}, \tag{16}$$

where the second equality holds for $k \in \{k_{\mathrm{s}}, k_{\mathrm{d2}}\}$. The failure probability associated with the estimation of $\langle Z_k \rangle$ (with $k \in K$) is either given by $\varepsilon_{Z,1}^k = \epsilon_{Z,1}^k$ or by $\varepsilon_{Z,1}^k = \epsilon_{Z,1}^k + \epsilon_{\mathrm{H},Z,1}^k$, depending again on which *lemma* (*2* or *3*) we apply. By employing the relation $p(k_{\mathrm{s}}|1) = p_{k_{\mathrm{s}}} p(1|k_{\mathrm{s}}) / p(1) = p_{k_{\mathrm{s}}} k_{\mathrm{s}} \mathrm{e}^{-k_{\mathrm{s}}} / p(1)$, we obtain a lower bound on μ_1, which only depends on known parameters

$$\begin{aligned} \mu_1 \geqslant & \ p\left(k_{\mathrm{s}} \middle| 1\right) S_{Z,1}^{\mathrm{L}} \\ \geqslant & \frac{p_{k_{\mathrm{s}}} k_{\mathrm{s}}^2 \mathrm{e}^{-k_{\mathrm{s}}}}{\left(k_{\mathrm{d1}} - k_{\mathrm{d2}}\right)\left(k_{\mathrm{s}} - k_{\mathrm{d1}} - k_{\mathrm{d2}}\right)} \left[\frac{\mathrm{e}^{k_{\mathrm{d1}}}}{p_{k_{\mathrm{d1}}}} \left\langle Z_{k_{\mathrm{d1}}}^- \right\rangle - \frac{\mathrm{e}^{k_{\mathrm{d2}}}}{p_{k_{\mathrm{d2}}}} \left\langle Z_{k_{\mathrm{d2}}}^+ \right\rangle \right. \\ & \left. + \frac{k_{\mathrm{d1}}^2 - k_{\mathrm{d2}}^2}{k_{\mathrm{s}}^2} \left(\frac{\mu_0^{\mathrm{L}}}{p\left(k_{\mathrm{s}} \wedge 0\right)} - \frac{\mathrm{e}^{k_{\mathrm{s}}} \left\langle Z_{k_{\mathrm{s}}}^+ \right\rangle}{p_{k_{\mathrm{s}}}} \right) \right] =: \mu_1^L. \end{aligned} \tag{17}$$

Therefore, we have that

$$m_1 \geqslant \mu_1^{\mathrm{L}} - \Delta_{Z,1} =: m_1^{\mathrm{L}}, \tag{18}$$

except with error probability $\varepsilon_{Z,1} = \sum_{n=0}^{1}(\varepsilon_{Z,n}^{k_{\mathrm{d1}}} + \varepsilon_{Z,n}^{k_{\mathrm{d2}}}) + \epsilon_{Z,1} + \varepsilon_{Z,1}^{k_{\mathrm{s}}}$, where the parameters $\varepsilon_{Z,0}^{k_{\mathrm{d1}}}$ and $\varepsilon_{Z,0}^{k_{\mathrm{d2}}}$ come from the estimation of μ_0^{L}.

4.2. Estimation of the number of vacuum and single-photon contributions for the intensity-fluctuation case

We now evaluate the scenario where the laser suffers from intensity fluctuations. As introduced above, here we shall assume that Alice only knows the range $[k^-, k^+]$ where the intensity value k lies. Below we introduce the final expressions for the different parameters; the detailed derivations are referred to appendix C.

4.2.1. Estimation of the number of vacuum contributions

Here, we present the result for the estimation of the lower bound on $T_{Z,0}$. Here, $T_{Z,0}$ is the sum of the conditional probability that Bob detects a signal in the Z basis conditioned that Alice chooses the signal intensity and sends a vacuum state in the Z basis (see equation (60)). It is given by

$$T_{Z,0} \geqslant \frac{1}{k_{\mathrm{d1}}^- - k_{\mathrm{d2}}^+}\left(\frac{k_{\mathrm{d1}}^- \mathrm{e}^{k_{\mathrm{d2}}^-}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle - \frac{k_{\mathrm{d2}}^+ \mathrm{e}^{k_{\mathrm{d1}}^+}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle\right) =: T_{Z,0}^{\mathrm{L}}. \tag{19}$$

To calculate the mean values $\langle Z_{k_{\mathrm{d1}}}\rangle$ and $\langle Z_{k_{\mathrm{d2}}}\rangle$ we employ Azuma's inequality, which is described in *Lemma 4* (see appendix B). Importantly, note that this inequality holds without assuming independence of the trials. As a result, we obtain a lower bound on $\langle Z_{k_{\mathrm{d1}}}\rangle$ together with an upper bound on $\langle Z_{k_{\mathrm{d2}}}\rangle$. They are given by

$$\left\langle Z_{k_{\mathrm{d2}}}^-\right\rangle := |Z_{k_{\mathrm{d2}}}| - g_{\mathrm{A}}\left(N_z, \epsilon_{Z,0}^{k_{\mathrm{d2}}}\right), \tag{20}$$

$$\left\langle Z_{k_{\mathrm{d1}}}^+\right\rangle := \left|Z_{k_{\mathrm{d1}}}\right| + g_{\mathrm{A}}\left(N_z, \epsilon_{Z,0}^{k_{\mathrm{d1}}}\right), \tag{21}$$

where $g_{\mathrm{A}}(x, y) = \sqrt{2x \ln(1/y)}$, and N_z is the number of events where Alice and Bob use the Z basis within N trials.

In so doing, we find a lower bound on μ_0 that only depends on parameters that are directly observed in the experiment. It has the form

$$\mu_0 \geqslant p^-\left(k_{\mathrm{s}} \wedge 0\right) T_{Z,0}^{\mathrm{L}} \geqslant \frac{p_{k_{\mathrm{s}}}\mathrm{e}^{-k_{\mathrm{s}}^+}}{k_{\mathrm{d1}}^- - k_{\mathrm{d2}}^+}\left(\frac{k_{\mathrm{d1}}^- \mathrm{e}^{k_{\mathrm{d2}}^-}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}^-\right\rangle - \frac{k_{\mathrm{d2}}^+ \mathrm{e}^{k_{\mathrm{d1}}^+}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}^+\right\rangle\right) =: \mu_0^{\mathrm{L}}, \tag{22}$$

where the $p^-(k_{\mathrm{s}} \wedge 0)$ is a lower bound on $p(k_{\mathrm{s}} \wedge 0)$.

Finally, we obtain a lower bound on m_0 which is given by

$$m_0 \geqslant \mu_0^{\mathrm{L}} - \Delta_{Z,0} =: m_0^{\mathrm{L}}, \tag{23}$$

except with error probability $\varepsilon_{Z,0} = \epsilon_{Z,0} + \epsilon_{Z,0}^{k_{\mathrm{d1}}} + \epsilon_{Z,0}^{k_{\mathrm{d2}}}$.

4.2.2. Estimation of the number of single-photon contributions

Here, we introduce a lower bound on $T_{Z,1}$. Here, $T_{Z,1}$ is the sum of the conditional probability that Bob detects a signal in the Z basis conditioned that Alice chooses the signal intensity and sends a single-photon state in the Z basis (see equation (69)).

It is given by

$$\begin{aligned} T_{Z,1} \geqslant \frac{k_{\mathrm{s}}^-}{\left(k_{\mathrm{d1}}^+ - k_{\mathrm{d2}}^-\right)\left(k_{\mathrm{s}}^- - k_{\mathrm{d1}}^+ - k_{\mathrm{d2}}^-\right)}&\left[\frac{\mathrm{e}^{k_{\mathrm{d1}}^-}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle - \frac{\mathrm{e}^{k_{\mathrm{d2}}^+}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle\right. \\ &\left. - \frac{\left(k_{\mathrm{d1}}^+\right)^2 - \left(k_{\mathrm{d2}}^-\right)^2}{\left(k_{\mathrm{s}}^-\right)^2}\left(\frac{\mathrm{e}^{k_{\mathrm{s}}^+}}{p_{k_{\mathrm{s}}}}\left\langle Z_{k_{\mathrm{s}}}\right\rangle - T_{Z,0}^{\mathrm{L}}\right)\right] =: T_{Z,1}^{\mathrm{L}}. \end{aligned} \tag{24}$$

Again, to estimate the mean values $\langle Z_{k_{\mathrm{d1}}}\rangle$, $\langle Z_{k_{\mathrm{d2}}}\rangle$ and $\langle Z_{k_{\mathrm{s}}}\rangle$ we employ *lemma 4*. This way we obtain a lower bound on $\langle Z_{k_{\mathrm{d1}}}\rangle$ and an upper bound on $\langle Z_{k_{\mathrm{d2}}}\rangle$ and $\langle Z_{k_{\mathrm{s}}}\rangle$ as

$$\langle Z_{k_{\mathrm{d1}}}^-\rangle := \left|Z_{k_{\mathrm{d1}}}\right| - g_{\mathrm{A}}\left(N_z, \epsilon_{Z,1}^{k_{\mathrm{d1}}}\right), \tag{25}$$

$$\langle Z_k^+\rangle := \left|Z_k\right| + g_{\mathrm{A}}\left(N_z, \epsilon_{Z,1}^{k}\right), \tag{26}$$

where the second equality holds for $k \in \{k_{\mathrm{s}}, k_{\mathrm{d2}}\}$.

Hence, a lower bound on μ_1 can be directly written as

$$\begin{aligned}\mu_1 &\geqslant p^-\left(k_\mathrm{s}\ \wedge\ 1\right)T_{Z,1}^\mathrm{L}\\ &\geqslant \frac{p_{k_\mathrm{s}}\mathrm{e}^{-k_\mathrm{s}^-}\left(k_\mathrm{s}^-\right)^2}{\left(k_\mathrm{d1}^+ - k_\mathrm{d2}^-\right)\left(k_\mathrm{s}^- - k_\mathrm{d1}^+ - k_\mathrm{d2}^-\right)}\left[\frac{\mathrm{e}^{k_\mathrm{d1}^-}}{p_{k_\mathrm{d1}}}\left\langle Z_{k_\mathrm{d1}}^-\right\rangle - \frac{\mathrm{e}^{k_\mathrm{d2}^+}}{p_{k_\mathrm{d2}}}\left\langle Z_{k_\mathrm{d2}}^+\right\rangle\right.\\ &\quad\left. - \frac{\left(k_\mathrm{d1}^+\right)^2 - \left(k_\mathrm{d2}^-\right)^2}{\left(k_\mathrm{s}^-\right)^2}\left(\frac{\mathrm{e}^{k_\mathrm{s}^+}}{p_{k_\mathrm{s}}}\left\langle Z_{k_\mathrm{s}}^+\right\rangle - \frac{\mu_0^\mathrm{L}}{p^-\left(k_\mathrm{s}\ \wedge\ 0\right)}\right)\right] =: \mu_1^\mathrm{L},\end{aligned} \tag{27}$$

where $p^-(k_\mathrm{s}\ \wedge\ 1)$ is a lower bound on $p(k_\mathrm{s}\ \wedge\ 1)$.

Finally, we obtain m_1^L as

$$m_1 \geqslant \mu_1^\mathrm{L} - \Delta_{Z,1} =: m_1^\mathrm{L}, \tag{28}$$

except with error probability $\varepsilon_{Z,1} = \sum_{n=0}^{1}(\epsilon_{Z,n}^{k_\mathrm{d1}} + \epsilon_{Z,n}^{k_\mathrm{d2}}) + \epsilon_{Z,1} + \epsilon_{Z,1}^{k_s}$.

4.3. Estimation of the number of phase errors

In this section we present an upper bound on N_ph, which is the number of phase errors in the single-photon emissions within the set Z_{k_s}. As already mentioned in section 2.1, the states sent by Alice are given by equation (1), and we assume that the distribution $p(\Delta\theta_\mathrm{A})$ is known to Alice. We denote the single-photon part of equation (1) as $\rho(\theta_\mathrm{A})$. Note that from equation (1) the state $\rho(\theta_\mathrm{A})$ can be written as $\rho(\theta_\mathrm{A}) = \int_0^{2\pi} p(\Delta\theta_\mathrm{A})P[(|1\rangle_\mathrm{r}|0\rangle_\mathrm{s} + \gamma\mathrm{e}^{\mathrm{i}(\theta_\mathrm{A}+\Delta\theta_\mathrm{A})}|0\rangle_\mathrm{r}|1\rangle_\mathrm{s})/\sqrt{1+\gamma^2}]\mathrm{d}\Delta\theta_\mathrm{A}$, where the parameter $\gamma = \sqrt{k^\mathrm{sig}/k^\mathrm{ref}}$ and the state $|n\rangle_{\mathrm{r(s)}}$ denotes an n-photon number state of the reference (signal) pulse. The state $\rho(\theta_\mathrm{A})$ can be expressed as a function of the Pauli operators as follows:

$$\begin{aligned}\rho\left(\theta_\mathrm{A}\right) = \int_0^{2\pi} p\left(\Delta\theta_\mathrm{A}\right)\frac{1}{2}&\left[\sigma_I + \frac{2\gamma}{1+\gamma^2}\left(\cos\left(\theta_\mathrm{A}+\Delta\theta_\mathrm{A}\right)\sigma_Z + \sin\left(\theta_\mathrm{A}+\Delta\theta_\mathrm{A}\right)\sigma_X\right)\right.\\ &\left.+\frac{1-\gamma^2}{1+\gamma^2}\sigma_Y\right]\mathrm{d}\Delta\theta_\mathrm{A}.\end{aligned} \tag{29}$$

Here we define the eigenvectors of the Pauli operators σ_Y, σ_Z and σ_X as: $|0_y\rangle = |1\rangle_\mathrm{r}|0\rangle_\mathrm{s}$, $|1_y\rangle = |0\rangle_\mathrm{r}|1\rangle_\mathrm{s}$, $|0_z\rangle = (|0_y\rangle + |1_y\rangle)/\sqrt{2}$, $|1_z\rangle = (-i\,|0_y\rangle + i\,|1_y\rangle)/\sqrt{2}$ and $|i_x\rangle = (|0_z\rangle + (-1)^i|1_z\rangle)/\sqrt{2}$ with $i \in \{0, 1\}$.

With this notation, the single-photon part of the three states sent by Alice can be expressed as $\rho_{0z} = \rho(0)$, $\rho_{1z} = \rho(\pi)$ and $\rho_{0x} = \rho(\pi/2)$. Let $\rho_S = (\sigma_I + \vec{\sigma}\cdot\vec{V_S})/2$, where $\vec{\sigma} = [\sigma_X, \sigma_Y, \sigma_Z]$ and the Bloch vector $\vec{V_S} = [V_X^S, V_Y, V_Z^S]$ is a real three-dimensional vector that satisfies $|\vec{V_S}| \leqslant 1$ with $S \in \{0z, 1z, 0x\}$. From [21] we have that if $V_Y \neq 0$ the phase error rate of ρ_{0z} and ρ_{1z} is equivalent to that obtained after the application of the following filter operation[10],

$$F_Y = \sqrt{1-V_Y}P\left[\left|0_y\right\rangle\right] + \sqrt{1+V_Y}P\left[\left|1_y\right\rangle\right]. \tag{30}$$

Note that the success probability $p = 1 - V_Y^2$ of this filter operation is the same for all the states that have the same V_Y. This means, in particular, that we can restrict ourselves to the estimation of the phase error rate of the states $\tilde{\rho}_S$ which lie in the σ_X–σ_Z plane

$$\tilde{\rho}_S := \frac{F_Y\rho_S F_Y^\dagger}{\mathrm{Tr}\left[F_Y^\dagger F_Y\rho_S\right]} = \frac{\left(\sigma_I + r_x^S\sigma_X + r_z^S\sigma_Z\right)}{2}, \tag{31}$$

where the parameters r_x^S and r_z^S are given by $r_x^S = V_X^S f(V_Y)$ and $r_z^S = V_Z^S f(V_Y)$ with $f(V_Y) = 1/\sqrt{1-V_Y^2}$. The states $\tilde{\rho}_S$ given by equation (31) can also be decomposed as

$$\tilde{\rho}_S = P_0^S P\left[\left|\phi_0^S\right\rangle\right] + P_1^S P\left[\left|\phi_1^S\right\rangle\right], \tag{32}$$

[10] Note that this filter operation is just a mathematical tool for the security analysis, and it does not need to be implemented in the actual experiments. It is mainly used to simplify the estimation of the transmission rates of some virtual states that are needed to calculate the phase error rate of the protocol (see appendix D). Such derivation could be performed as well without considering such filtered states, but the analysis is more cumbersome.

where the probabilities P_i^S have the form

$$P_i^S = \frac{1}{2}\left(1 - (-1)^i\sqrt{\left(r_x^S\right)^2 + \left(r_z^S\right)^2}\right), \tag{33}$$

and the eigenvectors $|\phi_i^S\rangle$ are given by

$$\left|\phi_i^S\right\rangle = \begin{cases} \dfrac{1}{\mathcal{N}}\left(\dfrac{r_z^S - (-1)^i\sqrt{\left(r_x^S\right)^2 + \left(r_z^S\right)^2}}{r_x^S}\left|0_z\right\rangle + \left|1_z\right\rangle\right) & \left(r_x^S \neq 0\right) \\ \left|i_z\right\rangle & \left(r_x^S = 0 \,\wedge\, r_z^S < 0\right) \\ \left|i \oplus 1_z\right\rangle & \left(r_x^S = 0 \,\wedge\, r_z^S > 0\right), \end{cases} \tag{34}$$

$$=: a_i^S\left|0_z\right\rangle + b_i^S\left|1_z\right\rangle, \tag{35}$$

for $i \in \{0, 1\}$, and where $\mathcal{N}$ is the normalization factor of the state.

After some lengthy calculations (see appendix D for details), we obtain that N_{ph} is upper bounded by

$$\begin{aligned} N_{\mathrm{ph}} \leqslant \sum_{s=0}^{1} & \frac{P(s+1)}{2\left\{1 + (-1)^s\left(\sqrt{P_0^{0z}P_0^{1z}}\left\langle \phi_0^{0z} \middle| \phi_0^{1z}\right\rangle + \sqrt{P_1^{0z}P_1^{1z}}\left\langle \phi_1^{0z} \middle| \phi_1^{1z}\right\rangle\right)\right\}}\Bigg[N_{M_{Xs}}(3) + N_{M_{Xs}}(4) \\ & +(-1)^s\sum_{t=0}^{1}\sqrt{P_t^{0z}P_t^{1z}}\left\{C_{t,0}N_{M_{Xs}}(3) + C_{t,1}N_{M_{Xs}}(4) + C_{t,2}N_{M_{Xs}}(5)\right\}\Bigg] + \Delta_{\mathrm{A},s+1}^{s\oplus 1} \\ =: {} & N_{\mathrm{ph}}^{\mathrm{U}}, \end{aligned} \tag{36}$$

except with error probability $\varepsilon_{\mathrm{ph}}$. Here, the terms $N_{M_{Xs}}(j)$ with $j \in \{3, 4, 5\}$ are defined in equations (96)–(98); the quantities $P(1)$ and $P(2)$ are given by equation (81); the parameters $C_{t,l}$ have the form $C_{t,l} := (a_t^{0z}a_t^{1z} + b_t^{0z}b_t^{1z})A_{0,l}^{-1} + (a_t^{0z}b_t^{1z} + b_t^{0z}a_t^{1z})A_{1,l}^{-1} + (a_t^{0z}a_t^{1z} - b_t^{0z}b_t^{1z})A_{2,l}^{-1}$ for $l \in \{0, 1, 2\}$; the coefficients $A_{i,j}^{-1}$ are the (i, j) element of the following matrix

$$A^{-1} := \frac{2}{Q}\begin{pmatrix} r_x^{1z}r_z^{0x} - r_x^{0x}r_z^{1z} & r_x^{0x}r_z^{0z} - r_x^{0z}r_z^{0x} & r_x^{0z}r_z^{1z} - r_x^{1z}r_z^{0z} \\ r_z^{1z} - r_z^{0x} & r_z^{0x} - r_z^{0z} & r_z^{0z} - r_z^{1z} \\ r_x^{0x} - r_x^{1z} & r_x^{0z} - r_x^{0x} & r_x^{0z} - r_x^{0x} \end{pmatrix}, \tag{37}$$

where $Q := r_x^{1z}(r_z^{0x} - r_z^{0z}) + r_x^{0x}(r_z^{0z} - r_z^{1z}) + r_x^{0z}(r_z^{1z} - r_z^{0x})$; and the fluctuation term $\Delta_{\mathrm{A},s+1}^{s\oplus 1}$ is given by equation (95).

5. Simulation of the key rate

In this section, we show the simulation result for a fibre-based QKD system. Alice chooses the intensity of the laser from the set $\{k_{\mathrm{s}}, k_{\mathrm{d1}}, k_{\mathrm{d2}}\}$, where we fix the intensity of the weakest decoy state to $k_{\mathrm{d2}} = 2 \times 10^{-4}$. This is so because, in practice, it is difficult to generate a vacuum state due to the imperfect extinction of the amplitude modulator. Also, we assume that Bob uses an active measurement setup with two single-photon detectors with detection efficiency $\eta_{\mathrm{det}} = 15\%$ and a dark count probability $p_{\mathrm{d}} = 5 \times 10^{-7}$. The attenuation coefficient of the optical fibre is 0.2 dB km^{-1} and its transmittance is $\eta_{\mathrm{ch}} = 10^{-0.2D/10}$ with D denoting the fibre length. The overall misalignment error of the optical system is fixed to be $e_{\mathrm{mis}} = 1\%$. In addition, we assume an error correction leakage $\lambda_{\mathrm{EC}} = f_{\mathrm{EC}}|Z_{k_{\mathrm{s}}}|h(e_z)$, where e_z is the bit error rate of the sifted key $(Z_{\mathrm{A}}, Z_{\mathrm{B}})$. Moreover, for simplicity, we consider that the error correction efficiency of the protocol is a constant number f_{EC}=1.16 which does not depend on the size of $Z_{k_{\mathrm{s}}}$. For simplicity, we model the imperfection of Alice's (Bob's) phase modulator as $\Delta\theta_{\mathrm{A}} = \xi\theta_{\mathrm{A}}/\pi$ $(\Delta\theta_{\mathrm{B}} = -\Delta\theta_{\mathrm{A}})$. Also, we consider that the intensity fluctuation of the laser source lies in the interval $[k^-, k^+]$ with $k^- = (1 - r)k$ and $k^+ = (1 + r)k$ for a fixed value r.

In these conditions, we simulate the secret key generation rate $R = \ell/N$ for a fixed value of the correctness coefficient $\epsilon_{\mathrm{c}} = 10^{-15}$. For this, we perform a numerical optimization of the resulting secure key rate over the free parameters p_z, $p_{k_{\mathrm{s}}}$, $p_{k_{\mathrm{d1}}}$, k_{s} and k_{d1}.

5.1. Key generation rate for the exact intensity control case

The resulting secret key rate for this scenario, i.e. when $r = 0$, is shown in figure 2. The security parameter is $\epsilon_{\mathrm{sec}} = 10^{-10}$ and the total number of signals sent by Alice is $N = 10^s$ with $s = 9, 10, 11$ and 12. We consider two possible cases: $\xi = 0$ (i.e., the perfect encoding case) and $\xi = 0.147$, which is equivalent to a phase

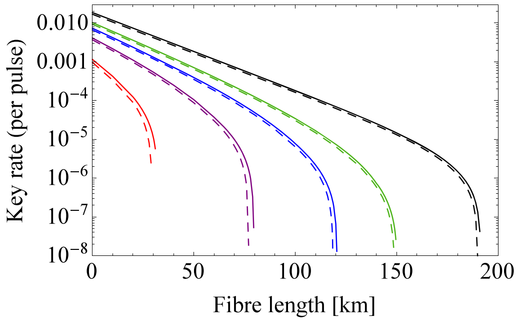

Figure 2. Secret key rate (per pulse) in logarithmic scale versus fibre length for the case with exact intensity control. The security parameter is $\epsilon_{\rm sec} = 10^{-10}$ and the total number of signals sent by Alice is $N = 10^s$ with $s = 9, 10, 11$ and 12 (from left to right). The rightmost two lines correspond to the asymptotic secret key rate with two decoy settings. The solid lines denote the case $\xi = 0$ (i.e., the perfect encoding scenario) while the dashed lines show the case $\xi = 0.147$ which is equivalent to a phase modulation error of 8.42° (this error parameter is measured in an updated version of a commercial plug&play system (ID Quantique Clavis 2) [28]). The experimental parameters are described in the main text.

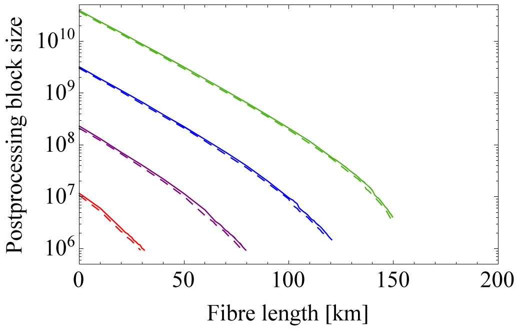

Figure 3. Postprocessing block size $|Z_{k_s}|$ versus fibre length for a fixed total number of signals $N = 10^s$ sent by Alice with exact intensity control, with $s = 9, 10, 11$ and 12 (from left to right). The solid lines correspond to the case $\xi = 0$ and the dashed lines are for $\xi = 0.147$.

modulation error of 8.42°. For comparison, figure 2 also includes the asymptotic secret key rate (i.e., the key rate in the limit of infinitely large keys) with two decoy settings.

As a result, we find that the effect of state preparation flaws on the key generation rate is almost negligible. Also, we have that if the total number of signals sent by Alice is about $N = 10^{12}$, Alice and Bob can exchange secret keys over 150 km both when $\xi = 0$ and $\xi = 0, 147$.

Finally, figure 3 shows the postprocessing block size $|Z_{k_s}|$ which is the length of the bit string to be processed in error correction and privacy amplification as a function of the distance when $N = 10^s$ with $s = 9, 10, 11$ and 12. This value is an essential parameter in actual experiments, as it gives us the length of the bit strings needed for the classical post-processing step of the protocol. As shown in figure 3, the size of $|Z_{k_s}|$ decreases linearly in logarithmic scale with the distance because the successful detection probability decreases exponentially with the distance.

5.2. Key generation rate for the intensity-fluctuation case

In this section we evaluate the resulting secret key rate when the laser source suffers from intensity fluctuations. We study two cases: $r = 0.02$ and $r = 0.05$, where r is the deviation rate from the expected value of the intensity. The results are shown in figures 4 and 6. Here we consider that $N = \{10^{14}, 10^{15}\}$, and the term ξ takes again the values $\xi = 0$ and $\xi = 0.147$. The security parameter is $\epsilon_{\rm sec} = 10^{-10}$ in figure 4 and $\epsilon_{\rm sec} = 10^{-8}$ in figure 6.

For comparison, these two figures also show the asymptotic secret key rate when Alice and Bob use two decoy settings. In this asymptotic case, we find that the degradation on the achievable key rate, when compared to the scenario $r = 0$, is only about 10 km (20 km) when $r = 0.02$ ($r = 0.05$).

In the finite-key regime, however, we obtain that the presence of intensity fluctuations seems to strongly limit the key generation rate if Alice and Bob do not know their probability distribution but only know the interval where the fluctuations lie in. For instance, when $N = 10^{11}$ and $r = 0$ (see figure 2) Alice and Bob can distribute a secret key over more than 100 km. However, to achieve a similar secret key rate performance when the intensity fluctuation of the source is 2% (i.e., the parameter $r = 0.02$) they need to exchange about $N = 10^{15}$

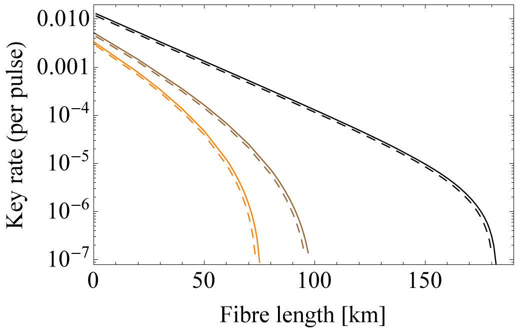

Figure 4. Secret key rate (per pulse) in logarithmic scale versus fibre length when the intensity fluctuation is 2%. The security parameter is $\epsilon_{\rm sec} = 10^{-10}$ and the total number of signals sent by Alice is $N = 10^s$ with $s = \{14, 15\}$ (from left to right). The rightmost two lines correspond to the asymptotic secret key rate with two decoy settings. The solid lines denote the case $\xi = 0$ (i.e., the perfect encoding scenario) while the dashed lines show the case $\xi = 0.147$ (which is equivalent to a phase modulation error of 8.42°). The experimental parameters are described in the main text.

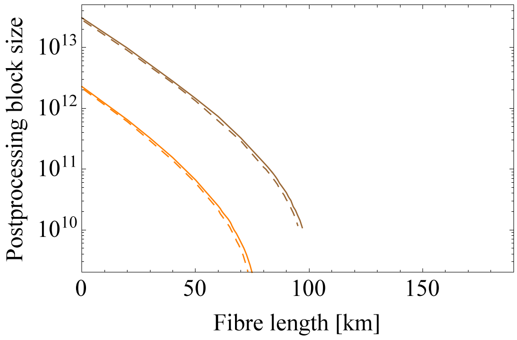

Figure 5. Postprocessing block size $|Z_{k_s}|$ versus fibre length for a fixed total number of signals $N = 10^s$ sent by Alice, with $s = \{14, 15\}$ when the intensity fluctuation is 2% (from left to right). The solid lines correspond to the case $\xi = 0$ and the dashed lines are for $\xi = 0.147$.

signals. The main technical reason for this behaviour seems to be the fact that Azuma's inequality [36] has a relatively slow convergence speed when compared to the Chernoff bound [34] and the Multiplicative Chernoff bound [13].

As a side remark, let us mention that when $r = 0.05$ and $N = 10^{14}$ we find that the achievable secret key rate is basically zero unless we increase the security parameter $\epsilon_{\rm sec}$ from $\epsilon_{\rm sec} = 10^{-10}$ to $\epsilon_{\rm sec} = 10^{-8}$. This is illustrated in figure 6.

Finally, figures 5 and 7 show the postprocessing block size $|Z_{k_s}|$ as a function of the distance when $N = 10^s$ with $s = \{14, 15\}$ for the 2% intensity fluctuation case and for the 5% intensity fluctuation case, respectively.

6. Conclusion

In summary, we have provided explicit security bounds for the loss-tolerant QKD protocol in the finite-key regime. On the application front, our results constitute an important step towards practical QKD with imperfect light sources, in that the resulting security performance is robust against encoding inaccuracies like, for instance, optical misalignments. Furthermore, our results take into account intensity fluctuations in the light source, which is a common experimental fact. Our results highlight the importance of the stable control of the intensity modulator as well as the need for a precise estimation of its intensity, which is not often sufficiently emphasized in the experiments. On a more general outlook, it would be of great practical interest to incorporate our results into measurement-device-independent QKD (mdiQKD) [11].

Acknowledgments

We thank Lo H-K, Xu F, Kato G, Azuma K, Ikuta R, Nagamatsu Y, Takeuchi Y and Matsuki K for valuable discussions on the security analysis and parameter estimation procedure, and Yoshino K, Fujiwara M, Sasaki M,

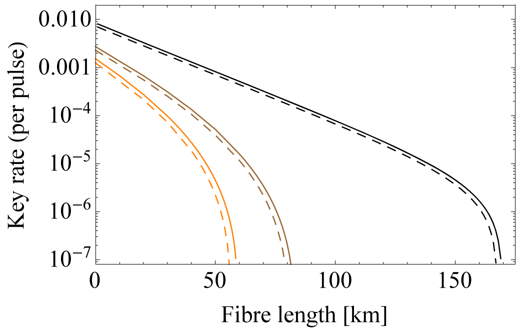

Figure 6. Secret key rate (per pulse) in logarithmic scale vs fibre length when the intensity fluctuation is 5%. The security parameter is $\epsilon_{\rm sec} = 10^{-8}$ and the total number of signals sent by Alice is $N = 10^s$ with $s = \{14, 15\}$ (from left to right). The rightmost two lines correspond to the asymptotic secret key rate with two decoy settings. The solid lines denote the case $\xi = 0$ (i.e., the perfect encoding scenario) while the dashed lines show the case $\xi = 0.147$ (which is equivalent to a phase modulation error of 8.42°). The experimental parameters are described in the main text.

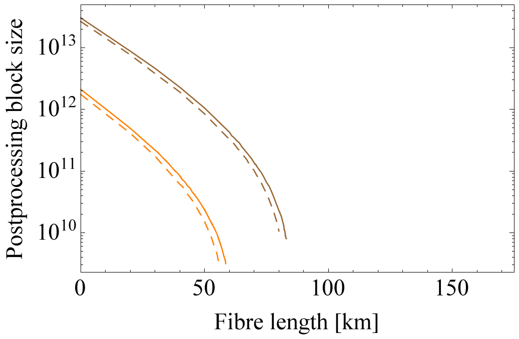

Figure 7. Postprocessing block size $|Z_{k_s}|$ vs fibre length for a fixed total number of signals $N = 10^s$ sent by Alice, with $s = \{14, 15\}$ when the intensity fluctuation is 5% (from left to right). The solid lines correspond to the case $\xi = 0$ and the dashed lines are for $\xi = 0.147$.

and Tomita A for fruitful discussions on practical QKD systems. AM acknowledges support from the JSPS Grant-in-Aid for Scientific Research(A) 25247068. MC thanks the Galician Regional Government (program ‘Ayudas para proyectos de investigacion desarrollados por investigadores emergentes’, and consolidation of Research Units: AtlantTIC), and the Spanish Government (project TEC2014-54898-R) for financial support. KT acknowledges support from the National Institute of Information and Communications Technology (NICT) of Japan (Project ‘Secure Photonic Network Technology’ as part of Project UQCC).

Appendix A. Derivation of the security bound

Here we present the calculations for the security bound given by equation (2). The security analysis is based on the universal composable security framework [30].

Recall that after privacy amplification, the joint state shared by Alice, Bob and Eve is described by the following classical-quantum state

$$\rho^{\rm actual}_{S_{\rm A}S_{\rm B}{\rm E}} = \sum_{s_{\rm A}, s_{\rm B}} p\left(s_{\rm A}, s_{\rm B}\right)\left|s_{\rm A}, s_{\rm B}\right\rangle\left\langle s_{\rm A}, s_{\rm B}\right|_{S_{\rm A}S_{\rm B}} \otimes \rho_{\rm E}^{s_{\rm A}, s_{\rm B}}, \tag{38}$$

where $s_{\rm A}$ and $s_{\rm B}$ are the classical bit strings for the keys, associated with orthonormal states $|s_{\rm A}\rangle$ and $|s_{\rm B}\rangle$ in a Hilbert space. Here, $p(s_{\rm A}, s_{\rm B})$ denotes the distribution of the keys and $\rho_{\rm E}^{s_{\rm A}, s_{\rm B}}$ is the quantum state of Eve's system conditioned on $S_{\rm A} = s_{\rm A}$ and $S_{\rm B} = s_{\rm B}$. In the ideal scenario, the joint state is described by

$$\rho^{\rm ideal}_{S_{\rm A}S_{\rm B}{\rm E}} = \frac{1}{2^{|s|}}\sum_{s} |s, s\rangle\langle s, s|_{S_{\rm A}S_{\rm B}} \otimes \rho_{\rm E}, \tag{39}$$

where $S_{\rm A} = S_{\rm B} = s$ and $\rho_{\rm E}$ is an arbitrary quantum state held by Eve. Using the security definition stated in the main text, a $\epsilon_{\rm sec}$-secure QKD protocol satisfies

$$\frac{1}{2}\left\|\rho^{\mathrm{actual}}_{\mathrm{S_A S_B E}}-\rho^{\mathrm{ideal}}_{\mathrm{S_A S_B E}}\right\|_1 \leqslant \epsilon_{\mathrm{sec}}. \tag{40}$$

Furthermore, if the security parameter ϵ_{sec} is appropriately chosen, it can be seen as the sum of errors in the correctness and secrecy, i.e., $\epsilon_{\mathrm{sec}} = \epsilon_{\mathrm{s}} + \epsilon_{\mathrm{c}}$. To see this, let us introduce an intermediate state

$$\rho^{\mathrm{inter}}_{\mathrm{S_A S_A E}} = \sum_{s_A} p\left(s_{\mathrm{A}}\right)\left|s_{\mathrm{A}}, s_{\mathrm{A}}\right\rangle\left\langle s_{\mathrm{A}}, s_{\mathrm{A}}\right|_{\mathrm{S_A S_A}} \otimes \rho^{s_{\mathrm{A}}}_{\mathrm{E}}, \tag{41}$$

which is just a trivial classical extension of Alice's state. Then, by using the triangle inequality property of the trace distance metric, we have

$$\frac{1}{2}\left\|\rho^{\mathrm{actual}}_{\mathrm{S_A S_B E}}-\rho^{\mathrm{ideal}}_{\mathrm{S_A S_B E}}\right\|_1 \leqslant \frac{1}{2}\left\|\rho^{\mathrm{actual}}_{\mathrm{S_A S_B E}}-\rho^{\mathrm{inter}}_{\mathrm{S_A S_A E}}\right\|_1 + \frac{1}{2}\left\|\rho^{\mathrm{inter}}_{\mathrm{S_A S_A E}}-\rho^{\mathrm{ideal}}_{\mathrm{S_A S_B E}}\right\|_1.$$

Fixing the first term on the rhs to ϵ_{c} gives

$$\epsilon_{\mathrm{c}} = \frac{1}{2}\left\|\rho^{\mathrm{actual}}_{\mathrm{S_A S_B E}}-\rho^{\mathrm{inter}}_{\mathrm{S_A S_A E}}\right\|_1 \geqslant \frac{1}{2}\left\|\rho^{\mathrm{actual}}_{\mathrm{S_A S_B}}-\rho^{\mathrm{inter}}_{\mathrm{S_A S_A}}\right\|_1 = \Pr\left[\mathrm{S_A} \neq \mathrm{S_B}\right],$$

where the inequality is due to the fact that the trace distance metric is contractive under any trace-preserving operation (in our case, the partial trace operation). Similarly, by fixing the second term to ϵ_{s} we have

$$\epsilon_{\mathrm{s}} = \frac{1}{2}\left\|\rho^{\mathrm{inter}}_{\mathrm{S_A S_A E}}-\rho^{\mathrm{ideal}}_{\mathrm{S_A S_B E}}\right\|_1 \geqslant \frac{1}{2}\left\|\rho^{\mathrm{inter}}_{\mathrm{S_A E}}-\rho^{\mathrm{ideal}}_{\mathrm{S_A E}}\right\|_1.$$

Therefore, fixing $\epsilon_{\mathrm{sec}} = \epsilon_{\mathrm{s}} + \epsilon_{\mathrm{c}}$ gives the desired decomposition.

From [32], the lower bound on the secret key length of our protocol is written as

$$\ell \geqslant \left\lfloor m_0^{\mathrm{L}} + m_1^{\mathrm{L}}[1-\Gamma] - \lambda_{\mathrm{EC}} - \log_2\frac{2}{\epsilon_{\mathrm{c}}}\right\rfloor, \tag{42}$$

where m_0^{L} and m_1^{L} are the lower bounds on the detection events of the vacuum and the single-photon emission, respectively, and $m_1^{\mathrm{L}}\Gamma = m_1^{\mathrm{L}}(h(e_{\mathrm{ph}}^{\mathrm{U}}) + \delta)$ is the number of rounds performing the random hashing to correct the phase error, which is equivalent to the number of bits sacrificed in the privacy amplification step of the protocol. The parameter λ_{EC} denotes the number of bits consumed in bit error correction, and $\left\lceil \log_2 1/\epsilon_{\mathrm{c}}\right\rceil \leqslant \log_2 2/\epsilon_{\mathrm{c}}$ is the length of the hash that Alice sends to Bob for the error verification using the universal$_2$ hash functions. From [7] and [33], we have that ϵ_{s} can be bounded by $\epsilon_{\mathrm{s}} \leqslant \sqrt{1-(1-\eta)(1-2^{-m_1^{\mathrm{L}}\delta+1})} \leqslant \sqrt{\eta + 2^{-m_1^{\mathrm{L}}\delta+1}}$. Therefore, the secret key length is obtained as

$$\ell \geqslant \left\lfloor m_0^{\mathrm{L}} + m_1^{\mathrm{L}}\left[1-h\left(e_{\mathrm{ph}}^{\mathrm{U}}\right)\right] - \log_2\frac{2}{\epsilon_{\mathrm{s}}^2-\eta} - \lambda_{\mathrm{EC}} - \log_2\frac{2}{\epsilon_{\mathrm{c}}}\right\rfloor, \tag{43}$$

where we consider η as a fixed value in this paper.

Appendix B. Technical lemmas

In this appendix we introduce four different concentration inequalities which are used throughout this paper. First, we introduce the stochastic model that is assumed in *lemmas*1, 2 and 3.

Stochastic model in lemmas 1, 2 and 3. Let X_1, X_2 ..., X_N be a set of independent Bernoulli random variables that satisfy $\mathrm{P}(X_i = 1) = p_i$, and let $X := \sum_{i=1}^N X_i$. The expected value of X is denoted as $\mu := E[X] = \sum_{i=1}^N p_i$. An observed outcome of X is represented as x.

Lemma 1. Chernoff bound [34].

This bound requires the knowledge of μ. It relates x with μ as

$$x = \mu + \delta_{\mathrm{C}}, \tag{44}$$

except with error probability $\epsilon_{\mathrm{C}} + \hat{\epsilon}_{\mathrm{C}}$, where the fluctuation term δ_{C} lies in the interval $\delta_{\mathrm{C}} \in [-\Delta_{\mathrm{C}}, \hat{\Delta}_{\mathrm{C}}]$ with $\Delta_{\mathrm{C}} = g_{\mathrm{C}}(\mu, \epsilon_{\mathrm{C}})$ and $\hat{\Delta}_{\mathrm{C}} = \hat{g}_{\mathrm{C}}(\mu, \hat{\epsilon}_{\mathrm{C}})$, where $g_{\mathrm{C}}(x, y) = \sqrt{2x \ln 1/y}$ and $\hat{g}_{\mathrm{C}}(x, y) = \sqrt{3x \ln 1/y}$. Here the parameter ϵ_{C} $(\hat{\epsilon}_{\mathrm{C}})$ denotes the probability that $x < \mu - \Delta_{\mathrm{C}}$ $(x > \mu + \hat{\Delta}_{\mathrm{C}})$. Equation (44) holds if both $0 < g_{\mathrm{C}}(1/\mu, \epsilon_{\mathrm{C}}) < 1$ and $0 < \hat{g}_{\mathrm{C}}(1/\mu, \hat{\epsilon}_{\mathrm{C}}) < 1$ are met.

Lemma 2. Hoeffding bound [35].

This bound does not require the knowledge of μ. It relates μ and x as

$$\mu = x + \delta_{\mathrm{H}}, \tag{45}$$

except with error probability $\epsilon_{\mathrm{H}} + \hat{\epsilon}_{\mathrm{H}}$, where the fluctuation term δ_{H} lies in the interval $\delta_{\mathrm{H}} \in [-\Delta_{\mathrm{H}}, \hat{\Delta}_{\mathrm{H}}]$ with $\Delta_{\mathrm{H}} = g_{\mathrm{H}}(N, \epsilon_{\mathrm{H}})$ and $\hat{\Delta}_{\mathrm{H}} = g_{\mathrm{H}}(N, \hat{\epsilon}_{\mathrm{H}})$, and where $g_{\mathrm{H}}(x, y) = \sqrt{x/2 \ln 1/y}$.

Lemma 3. Multiplicative Chernoff bound [13].

This bound does not require the knowledge of μ. It combines *lemmas 1* and *2* above. It uses *Lemma 2* to estimate a lower bound on μ that is then basically used in combination with *lemma 1*. In particular, let $\mu_{\rm L} = x - \sqrt{N/2 \ln 1/\epsilon_{\rm H}}$ for certain $\epsilon_{\rm H} > 0$. Then, if the following two conditions are satisfied: $(2\hat{\epsilon}_{\rm M}^{-1})^{1/\mu_{\rm L}} \leqslant \exp(9/32)$ and $\epsilon_{\rm M}^{-1/\mu_{\rm L}} < \exp(1/3)$ with $\hat{\epsilon}_{\rm M},\ \epsilon_{\rm M} > 0$, this lemma states that μ and x can be related as

$$\mu = x + \delta_{\rm M}, \tag{46}$$

except with error probability $\epsilon_{\rm H} + \epsilon_{\rm M} + \hat{\epsilon}_{\rm M}$, where $\delta_{\rm M}$ lies in the interval $[-\Delta_{\rm M}, \hat{\Delta}_{\rm M}]$ with $\hat{\Delta}_{\rm M} = g_{\rm M}(x, \hat{\epsilon}_{\rm M}^4/16)$ and $\Delta_{\rm M} = g_{\rm M}(x, \epsilon_{\rm M}^{3/2})$, and where $g_{\rm M}(x, y) = \sqrt{2x \ln(y^{-1})}$.

Lemma 4. Azuma's inequality [36, 37].

Note that *lemmas 1, 2* and *3* apply only to independent random variables, however, Azuma's inequality is applicable to any random variables (including dependent ones, i.e., random variables which can be correlated in any way) as long as two particular conditions (i.e., a Martingale and a Bounded difference condition (BDC), see below) are satisfied. In general, Eve's attacks can be coherent attacks, i.e., Eve can first make all the pulses sent by Alice to interact in a coherent way with an ancilla system in her hands and then measure the ancilla only after she has learned all the information distributed by Alice and Bob through the classical channel. In this general scenario, therefore, one cannot assume that each sending pulse is independent of each other. Hence, in order to analyse the security of the loss-tolerant protocol against coherent attacks in the finite-key regime, we use Azuma's inequality.

In particular, a sequence of random variables $X^{(0)}, X^{(1)}, \ldots$ is called a Martingale if and only if $E[X^{(l+1)}|X^{(0)}, X^{(1)}, \ldots, X^{(l)}] = X^{(l)}$ for all non-negative integer l, where $E[\,\cdot\,]$ represents the expectation value. On the other hand, $X^{(0)}, X^{(1)}, \ldots$ is said to fulfil the BDC if there exists $c^{(l)} > 0$ such that $|X^{(l+1)} - X^{(l)}| \leqslant c^{(l)}$ for all non-negative integer l.

Let us consider N trials of a random variable $X^{(l)}$, where l refers to the lth trial. If $X^{(l)}$ is a Martingale and satisfies the BDC with $c^{(l)} = 1$ then Azuma's inequality guarantees that

$$\Pr\left[\left|X^{(N)} - X^{(0)}\right| > N\delta\right] \leqslant 2{\rm e}^{-\frac{N\delta^2}{2}} \tag{47}$$

for any $\delta \in (0, 1)$.

Let us now define the following random variable for the lth trial

$$X^{(l)} := \Lambda^{(l)} - \sum_{u=1}^{l} P\left(u\,|\xi_0, \ldots, \xi_{u-1}\right), \tag{48}$$

where $\Lambda^{(l)}$ represents the actual number of events of the form $X^{(l)} = 1$ observed amongst the first l trials, and $P(u|\xi_0, \ldots, \xi_{u-1})$ is the conditional probability of having the event '1' in the uth trial conditioned on the first $u - 1$ outcomes $\xi_0, \ldots, \xi_{u-1}$. In this scenario, it is straightforward to show that the random variables given by equation (48) are Martingale and satisfy the BDC with $c^{(l)} = 1$. Hence, by applying Azuma's inequality we have that

$$\Pr\left[\left|\Lambda^{(N)} - \sum_{u=1}^{N} P\left(u\,|\xi_0, \ldots, \xi_{u-1}\right)\right| > N\delta\right] \leqslant 2{\rm e}^{-\frac{N\delta^2}{2}}. \tag{49}$$

This means, in particular, that

$$\Lambda^{(N)} = \sum_{u=1}^{N} P\left(u\middle|\xi_0, \ldots, \xi_{u-1}\right) + \delta_{\rm A} \tag{50}$$

except with error probability $\epsilon_{\rm A} + \hat{\epsilon}_{\rm A}$, where the parameter $\delta_{\rm A}$ lies in the interval $\delta_{\rm A} \in [-\Delta_{\rm A}, \hat{\Delta}_{\rm A}]$ with $\Delta_{\rm A} = g_{\rm A}(N, \epsilon_{\rm A})$ and $\hat{\Delta}_{\rm A} = g_{\rm A}(N, \hat{\epsilon}_{\rm A})$, and where $g_{\rm A}(x, y) = \sqrt{2x \ln(1/y)}$.

Appendix C. Decoy-state analysis

In this appendix we first present the detail of the decoy-state analysis for the intensity fluctuation case and then we summarize all the equations for the decoy-state analysis, including those for the exact intensity control case. More precisely, we describe the estimation procedure that we use in order to obtain a lower bound on the number of vacuum contributions $T_{Z,0}$, and both a lower and an upper bound on the number of single-photon contributions $T_{Z,1}$.

C.1. Intensity fluctuation case

Here, we generalize the decoy-state method to cover the case where the source suffers from intensity fluctuations. For this, as already mentioned previously, we shall consider that Alice and Bob only know the interval $[k^-, k^+]$ where the intensity k lies.

We begin by calculating the mean value $\langle Z_k \rangle$. Our starting point is the random variable $X_k^{\left(i\middle|\overrightarrow{i-1}\right)}$ for the ith trial when both Alice and Bob select the Z basis. This random variable takes the value 1 if Alice chooses the intensity k and, moreover, the generated signal is detected by Bob; otherwise it is 0. The term $\overrightarrow{i-1}$ reflects the fact that $X_k^{\left(i\middle|\overrightarrow{i-1}\right)}$ may depend on all the previous $i-1$ trials. With this notation, $\langle Z_k \rangle$ can be expressed as

$$\langle Z_k \rangle = \sum_{i=1}^{N_z} E\left[X_k^{\left(i\middle|\overrightarrow{i-1}\right)}\right] = \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(k \wedge \det|Z), \tag{51}$$

where N_z is the number of events where both Alice and Bob select the Z basis. The probability $p^{\left(i\middle|\overrightarrow{i-1}\right)}(*)$ denotes the conditional probability that the event $*$ occurs in the ith trial conditioned on the results obtained in the previous $i-1$ trials, and the term $k \wedge \det|Z$ represents the event where Alice selects the intensity k and Bob detects the generated signal given that both of them have chosen the Z basis. By using Bayes rule, we can rewrite equation (51) as

$$\langle Z_k \rangle = \frac{1}{p_z^2} \sum_{i=1}^{N_z} \sum_{n=0}^{\infty} p^{\left(i\middle|\overrightarrow{i-1}\right)}(k \wedge Z \wedge n \wedge \det), \tag{52}$$

$$= \frac{1}{p_z^2} \sum_{i=1}^{N_z} \sum_{n=0}^{\infty} p^{(i)}(k \wedge Z \wedge n) p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|k \wedge Z \wedge n), \tag{53}$$

$$= p_k \sum_{i=1}^{N_z} \sum_{n=0}^{\infty} p^{(i)}(n|k \wedge Z) p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|Z \wedge n), \tag{54}$$

where p_k is the probability that Alice chooses the intensity k; n denotes an n-photon signal; p_z represents the probability of selecting the Z basis; and $p^{(i)}(\,*\,)$ is the probability that the event $*$ occurs in the ith trial. For instance, $p^{(i)}(n|k \wedge Z)$ is the conditional probability that Alice emits an n-photon state in the ith trial given that she has chosen the intensity k and both Alice and Bob have selected the Z basis in the ith trial. Note that in the transformation from equation (53) to (54) we have used the property of the decoy-state method i.e., $p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|k \wedge Z \wedge n) = p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|Z \wedge n)$.

In so doing, we obtain that $\langle Z_k \rangle$ is upper bounded by

$$\langle Z_k \rangle \leqslant p_k \sum_{i=1}^{N_z} \sum_{n=0}^{\infty} \frac{e^{-k^-}\left(k^+\right)^n}{n!} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|Z \wedge n). \tag{55}$$

Similarly, we find that

$$\langle Z_k \rangle \geqslant p_k \sum_{i=1}^{N_z} \sum_{n=0}^{\infty} \frac{e^{-k^+}\left(k^-\right)^n}{n!} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|Z \wedge n). \tag{56}$$

Lower bound on the number of vacuum contributions.

To obtain this bound, we first rewrite equations (55) and (56) for the cases $k = k_{d2}$ and $k = k_{d1}$, respectively. We obtain the following two inequalities

$$\begin{aligned} \frac{e^{k_{d2}^-}}{p_{k_{d2}}} \left\langle Z_{k_{d2}} \right\rangle \leqslant & \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|0 \wedge Z) + \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|1 \wedge Z) k_{d2}^+ \\ & + \sum_{i=1}^{N_z} \sum_{n \geqslant 2} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|n \wedge Z) \frac{\left(k_{d2}^+\right)^n}{n!}. \end{aligned} \tag{57}$$

$$\begin{aligned} \frac{e^{k_{d1}^+}}{p_{k_{d1}}} \left\langle Z_{k_{d1}} \right\rangle \geqslant & \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|0 \wedge Z) + \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|1 \wedge Z) k_{d1}^- \\ & + \sum_{i=1}^{N_z} \sum_{n \geqslant 2} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|n \wedge Z) \frac{\left(k_{d1}^-\right)^n}{n!}, \end{aligned} \tag{58}$$

Next, we multiply equation (57) by k_{d1}^- and equation (58) by k_{d2}^+, and we add both expressions. In so doing, we find that

$$\begin{aligned}\left(k_{\mathrm{d1}}^- - k_{\mathrm{d2}}^+\right)\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|0\ \wedge\ Z) &\geqslant \frac{k_{\mathrm{d1}}^-\mathrm{e}^{k_{\mathrm{d2}}^-}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle - \frac{k_{\mathrm{d2}}^+\mathrm{e}^{k_{\mathrm{d1}}^+}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle\\ &\quad + k_{\mathrm{d1}}^- k_{\mathrm{d2}}^+\sum_{i=1}^{N_z}\sum_{n\geqslant 2}\frac{\left(k_{\mathrm{d1}}^-\right)^{n-1} - \left(k_{\mathrm{d2}}^+\right)^{n-1}}{n!} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|n\ \wedge\ Z)\\ &\geqslant k_{\mathrm{d1}}^-\frac{\mathrm{e}^{k_{\mathrm{d2}}^-}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle - k_{\mathrm{d2}}^+\frac{\mathrm{e}^{k_{\mathrm{d1}}^+}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle, \end{aligned} \tag{59}$$

where the second inequality holds because $k_{\mathrm{d1}}^- > k_{\mathrm{d2}}^+$.

As a result, we find that $T_{Z,0}$ is lower bounded by

$$T_{Z,0} \coloneqq \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|0\ \wedge\ Z) \geqslant \frac{1}{k_{\mathrm{d1}}^- - k_{\mathrm{d2}}^+}\left(k_{\mathrm{d1}}^-\frac{\mathrm{e}^{k_{\mathrm{d2}}^-}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle - k_{\mathrm{d2}}^+\frac{\mathrm{e}^{k_{\mathrm{d1}}^+}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle\right). \tag{60}$$

To estimate the expectation values $\langle Z_{k_{\mathrm{d1}}}\rangle$ and $\langle Z_{k_{\mathrm{d2}}}\rangle$, we use Azuma's inequality because each trial of the random variables $X_{k_{\mathrm{d1}}}^{\left(i\middle|\overrightarrow{i-1}\right)}$ and $X_{k_{\mathrm{d2}}}^{\left(i\middle|\overrightarrow{i-1}\right)}$ may depend on the previous ones.

Lower bound on the number of single-photon contributions.

Here, we first particularize equations (55) and (56) for the cases $k = k_{\mathrm{d1}}$ and $k = k_{\mathrm{d2}}$, respectively. We have that

$$\begin{aligned}\frac{\mathrm{e}^{k_{\mathrm{d1}}^-}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle &\leqslant \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|0\ \wedge\ Z) + \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|1\ \wedge\ Z)\left(k_{\mathrm{d1}}^+\right)\\ &\quad + \sum_{n\geqslant 2}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|n\ \wedge\ Z)\frac{\left(k_{\mathrm{d1}}^+\right)^n}{n!}. \end{aligned} \tag{61}$$

$$\begin{aligned}\frac{\mathrm{e}^{k_{\mathrm{d2}}^+}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle &\geqslant \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|0\ \wedge\ Z) + \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|1\ \wedge\ Z)\left(k_{\mathrm{d2}}^-\right)\\ &\quad + \sum_{n\geqslant 2}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|n\ \wedge\ Z)\frac{\left(k_{\mathrm{d2}}^-\right)^n}{n!}, \end{aligned} \tag{62}$$

Next, we add both expressions and we obtain

$$\begin{aligned}&\frac{\mathrm{e}^{k_{\mathrm{d2}}^+}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle + \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|1\ \wedge\ Z)\left(k_{\mathrm{d1}}^+\right) + \sum_{n\geqslant 2}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|n\ \wedge\ Z)\frac{\left(k_{\mathrm{d1}}^+\right)^n}{n!}\\ &\geqslant \frac{\mathrm{e}^{k_{\mathrm{d1}}^-}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle + \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|1\ \wedge\ Z)\left(k_{\mathrm{d2}}^-\right) + \sum_{n\geqslant 2}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|n\ \wedge\ Z)\frac{\left(k_{\mathrm{d2}}^-\right)^n}{n!}. \end{aligned} \tag{63}$$

This last equation can be rewritten as

$$\begin{aligned}\left(k_{\mathrm{d1}}^+ - k_{\mathrm{d2}}^-\right)\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|1\ \wedge\ Z) &\geqslant \frac{\mathrm{e}^{k_{\mathrm{d1}}^-}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle - \frac{\mathrm{e}^{k_{\mathrm{d2}}^+}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle\\ &\quad + \sum_{n\geqslant 2}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|n\ \wedge\ Z)\frac{\left(k_{\mathrm{d2}}^-\right)^n - \left(k_{\mathrm{d1}}^+\right)^n}{n!}. \end{aligned} \tag{64}$$

Next, we evaluate the third term on the rhs of equation (64). This term is lower bounded by

$$\begin{aligned}&\sum_{n\geqslant 2}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|n\ \wedge\ Z)\frac{\left(k_{\mathrm{d2}}^-\right)^n - \left(k_{\mathrm{d1}}^+\right)^n}{n!}\\ &\geqslant \frac{\left(k_{\mathrm{d2}}^-\right)^2 - \left(k_{\mathrm{d1}}^+\right)^2}{\left(k_{\mathrm{s}}^-\right)^2}\sum_{n\geqslant 2}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\det|n\ \wedge\ Z)\frac{\left(k_{\mathrm{s}}^-\right)^n}{n!}, \end{aligned} \tag{65}$$

because when the conditions $n \geqslant 2$, $k_{\mathrm{d1}}^+ > k_{\mathrm{d2}}^-$ and $k_{\mathrm{s}}^- > k_{\mathrm{d1}}^+ + k_{\mathrm{d2}}^-$ are satisfied we have that $(k_{\mathrm{d2}}^-)^n - (k_{\mathrm{d1}}^+)^n \geqslant [(k_{\mathrm{d2}}^-)^2 - (k_{\mathrm{d1}}^+)^2](k_{\mathrm{s}}^-)^{n-2}$. If we now use equation (56) for $k = k_{\mathrm{s}}$, we have that

$$\begin{aligned}\sum_{n\geqslant 2}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|n\,\wedge\,Z)\frac{\left(k_{\mathrm{s}}^{-}\right)^{n}}{n!} \leqslant{}& \frac{\mathrm{e}^{k_{\mathrm{s}}^{+}}}{p_{k_{\mathrm{s}}}}\left\langle Z_{k_{\mathrm{s}}}\right\rangle\\ &-\sum_{i=1}^{N_z}\left(p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|0\,\wedge\,Z)+k_{\mathrm{s}}^{-}p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|1\,\wedge\,Z)\right).\end{aligned}\tag{66}$$

The rhs of equation (65) can be lower bounded using the rhs of equation (66). This is so because $k_{\mathrm{d1}}^{+} > k_{\mathrm{d2}}^{-}$ and therefore the term $[(k_{\mathrm{d2}}^{-})^2 - (k_{\mathrm{d1}}^{+})^2]/(k_{\mathrm{s}}^{-})^2 < 0$ in equation (65). Hence, we have that the third term on the rhs of equation (64) is lower bounded by

$$\begin{aligned}\sum_{n\geqslant 2}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|n\,\wedge\,Z)\frac{\left(k_{\mathrm{d2}}^{-}\right)^{n}-\left(k_{\mathrm{d1}}^{+}\right)^{n}}{n!} \geqslant{}& \frac{\left(k_{\mathrm{d2}}^{-}\right)^{2}-\left(k_{\mathrm{d1}}^{+}\right)^{2}}{\left(k_{\mathrm{s}}^{-}\right)^{2}}\left[\frac{\mathrm{e}^{k_{\mathrm{s}}^{+}}}{p_{k_{\mathrm{s}}}}\left\langle Z_{k_{\mathrm{s}}}\right\rangle\right.\\ &\left.-\sum_{i=1}^{N_z}\left(p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|0\,\wedge\,Z)+k_{\mathrm{s}}^{-}p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|1\,\wedge\,Z)\right)\right].\end{aligned}\tag{67}$$

That is, if we now combine equations (64) and (67) we find that

$$\begin{aligned}\left(k_{\mathrm{d1}}^{+}-k_{\mathrm{d2}}^{-}\right)\left\{\frac{k_{\mathrm{s}}^{-}-\left(k_{\mathrm{d1}}^{+}+k_{\mathrm{d2}}^{-}\right)}{k_{\mathrm{s}}^{-}}\right\}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|1\,\wedge\,Z) \geqslant{}& \frac{\mathrm{e}^{k_{\mathrm{d1}}^{-}}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle-\frac{\mathrm{e}^{k_{\mathrm{d2}}^{+}}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle\\ &-\frac{\left(k_{\mathrm{d1}}^{+}\right)^{2}-\left(k_{\mathrm{d2}}^{-}\right)^{2}}{\left(k_{\mathrm{s}}^{-}\right)^{2}}\left(\frac{\mathrm{e}^{k_{\mathrm{s}}^{+}}}{p_{k_{\mathrm{s}}}}\left\langle Z_{k_{\mathrm{s}}}\right\rangle-T_{Z,0}^{\mathrm{L}}\right),\end{aligned}\tag{68}$$

which directly gives us a lower bound on $T_{Z,1}$,

$$\begin{aligned}T_{Z,1} :={}& \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|1\,\wedge\,Z)\\ \geqslant{}& \frac{k_{\mathrm{s}}^{-}}{\left(k_{\mathrm{d1}}^{+}-k_{\mathrm{d2}}^{-}\right)\left(k_{\mathrm{s}}^{-}-k_{\mathrm{d1}}^{+}-k_{\mathrm{d2}}^{-}\right)}\left[\frac{\mathrm{e}^{k_{\mathrm{d1}}^{-}}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle-\frac{\mathrm{e}^{k_{\mathrm{d2}}^{+}}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle\right.\\ &\left.-\frac{\left(k_{\mathrm{d1}}^{+}\right)^{2}-\left(k_{\mathrm{d2}}^{-}\right)^{2}}{\left(k_{\mathrm{s}}^{-}\right)^{2}}\left(\frac{\mathrm{e}^{k_{\mathrm{s}}^{+}}}{p_{k_{\mathrm{s}}}}\left\langle Z_{k_{\mathrm{s}}}\right\rangle-T_{Z,0}^{\mathrm{L}}\right)\right].\end{aligned}\tag{69}$$

Here, the lower bound on $\langle Z_{k_{\mathrm{d1}}}\rangle$ and the upper bound on $\langle Z_{k_{\mathrm{s}}}\rangle$ and $\langle Z_{k_{\mathrm{d2}}}\rangle$ are estimated using Azuma's inequality. *Upper bound on the number of single-photon contributions.*

By adding equations (57) and (58), we have that

$$\begin{aligned}\left(k_{\mathrm{d1}}^{-}-k_{\mathrm{d2}}^{+}\right)\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|1\,\wedge\,Z) \leqslant{}& \frac{\mathrm{e}^{k_{\mathrm{d1}}^{+}}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle\\ &-\frac{\mathrm{e}^{k_{\mathrm{d2}}^{-}}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle+\sum_{n\geqslant 2}\sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|n\,\wedge\,Z)\frac{\left(k_{\mathrm{d2}}^{+}\right)^{n}-\left(k_{\mathrm{d1}}^{-}\right)^{n}}{n!}\\ \leqslant{}& \frac{\mathrm{e}^{k_{\mathrm{d1}}^{+}}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle-\frac{\mathrm{e}^{k_{\mathrm{d2}}^{-}}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle,\end{aligned}\tag{70}$$

where the second inequality holds because $k_{\mathrm{d1}}^{-} > k_{\mathrm{d2}}^{+}$. This means, in particular, that $T_{Z,1}$ is upper bounded by

$$T_{Z,1} = \sum_{i=1}^{N_z} p^{\left(i\middle|\overrightarrow{i-1}\right)}(\mathrm{det}|1\,\wedge\,Z) \leqslant \frac{1}{k_{\mathrm{d1}}^{-}-k_{\mathrm{d2}}^{+}}\left(\frac{\mathrm{e}^{k_{\mathrm{d1}}^{+}}}{p_{k_{\mathrm{d1}}}}\left\langle Z_{k_{\mathrm{d1}}}\right\rangle-\frac{\mathrm{e}^{k_{\mathrm{d2}}^{-}}}{p_{k_{\mathrm{d2}}}}\left\langle Z_{k_{\mathrm{d2}}}\right\rangle\right),\tag{71}$$

where the upper bound on $\langle Z_{k_{\mathrm{d1}}}\rangle$ and the lower bound on $\langle Z_{k_{\mathrm{d2}}}\rangle$ are estimated using Azuma's inequality.

C.2. Summary of the decoy-state analysis

Here, we summarize all the equations needed in the decoy-state method, including those for the exact intensity control case.

Lower bound on the number of vacuum contributions.

Let $\underline{\mathrm{Decoy}}_0(ay,\ by')$ denote a lower bound on the number of events where Alice generates a vacuum state using the signal intensity and the basis setting $a \in \{Z,\ X\}$ to encode a bit value $y \in \{0,\ 1\}$, and Bob observes the bit value $y' \in \{0,\ 1\}$ when he measures the received signal using the basis $b \in \{Z,\ X\}$.

$$\underline{\mathrm{Decoy}}_0(ay,\ by') = \frac{p^-\left(k_\mathrm{s}\ \wedge\ 0\right)}{k_{\mathrm{d}1}^- - k_{\mathrm{d}2}^+}\left(\frac{k_{\mathrm{d}1}^-\mathrm{e}^{k_{\mathrm{d}2}^-}}{p_{k_{\mathrm{d}2}}}\left\langle a^y b_{k_{\mathrm{d}2}}^{y'\ -}\right\rangle - \frac{k_{\mathrm{d}2}^+\mathrm{e}^{k_{\mathrm{d}1}^+}}{p_{k_{\mathrm{d}1}}}\left\langle a^y b_{k_{\mathrm{d}1}}^{y'\ +}\right\rangle\right), \tag{72}$$

where the parameters $\langle a^y b_{k_{\mathrm{d}2}}^{y'\ -}\rangle$ and $\langle a^y b_{k_{\mathrm{d}1}}^{y'\ +}\rangle$ are defined in a similar way like equations (9) and (10) for the exact intensity control case and like equations (20) and (21) for the intensity-fluctuation case, respectively. The probability $p^-(k_\mathrm{s}\ \wedge\ 0)$ is a lower bound on $p(k_\mathrm{s}\ \wedge\ 0)$ which denotes the probability that Alice selects the signal intensity setting and sends a vacuum state.

Lower bound on the number of single-photon contributions.

Let $\underline{\mathrm{Decoy}}_1(ay,\ by')$ denote a lower bound on the number of events where Alice prepares a single-photon state using the signal intensity and the basis setting $a \in \{Z,\ X\}$ to encode a bit value $y \in \{0,\ 1\}$, and Bob observes the bit value $y' \in \{0,\ 1\}$ when he measures the received signal using the basis $b \in \{Z,\ X\}$.

$$\begin{aligned}\underline{\mathrm{Decoy}}_1(ay,\ by') = \frac{p^-\left(k_\mathrm{s}\ \wedge\ 1\right)k_\mathrm{s}^-}{\left(k_{\mathrm{d}1}^+ - k_{\mathrm{d}2}^-\right)\left(k_\mathrm{s}^- - k_{\mathrm{d}1}^+ - k_{\mathrm{d}2}^-\right)}&\left[\frac{\mathrm{e}^{k_{\mathrm{d}1}^-}}{p_{k_{\mathrm{d}1}}}\left\langle a^y b^{y'}{}_{k_{\mathrm{d}1}}^{-}\right\rangle - \frac{\mathrm{e}^{k_{\mathrm{d}2}^+}}{p_{k_{\mathrm{d}2}}}\left\langle a^y b_{k_{\mathrm{d}2}}^{y'\ +}\right\rangle\right.\\ &\left.+\frac{\left(k_{\mathrm{d}1}^+\right)^2 - \left(k_{\mathrm{d}2}^-\right)^2}{\left(k_\mathrm{s}^-\right)^2}\left(\frac{\underline{\mathrm{Decoy}}_0(ay,\ by')}{p^-\left(k_\mathrm{s}\ \wedge\ 0\right)} - \frac{\mathrm{e}^{k_\mathrm{s}}\left\langle a^y b_{k_\mathrm{s}}^{y'+}\right\rangle}{p_{k_\mathrm{s}}}\right)\right],\end{aligned} \tag{73}$$

where the probability $p^-(k_\mathrm{s}\ \wedge\ 1)$ is a lower bound on $p(k_\mathrm{s}\ \wedge\ 1)$ which denotes the probability that Alice selects the signal intensity setting and sends a single-photon state.

Upper bound on the number of single-photon contributions.

Let $\overline{\mathrm{Decoy}}_1(ay,\ by')$ denote an upper bound on the number of events where Alice prepares a single-photon state using the signal intensity and the basis setting $a \in \{Z,\ X\}$ to encode a bit value $y \in \{0,\ 1\}$, and Bob observes the bit value $y' \in \{0,\ 1\}$ when he measures the received signal using the basis $b \in \{Z,\ X\}$.

$$\overline{\mathrm{Decoy}}_1(ay,\ by') = \frac{p^+\left(k_\mathrm{s}\ \wedge\ 1\right)}{k_{\mathrm{d}1}^- - k_{\mathrm{d}2}^+}\left(\frac{\mathrm{e}^{k_{\mathrm{d}1}^+}}{p_{k_{\mathrm{d}1}}}\left\langle a^y b_{k_{\mathrm{d}1}}^{y'\ +}\right\rangle - \frac{\mathrm{e}^{k_{\mathrm{d}2}^-}}{p_{k_{\mathrm{d}2}}}\left\langle a^y b_{k_{\mathrm{d}2}}^{y'\ -}\right\rangle\right), \tag{74}$$

where the probability $p^+(k_\mathrm{s}\ \wedge\ 1)$ is an upper bound on $p(k_\mathrm{s}\ \wedge\ 1)$.

Appendix D. Phase error rate estimation

In this appendix we explain how to derive equation (36). That is, we obtain an upper bound on the number of phase errors associated to the single-photon pulses emitted by Alice when she selects the signal intensity setting, both Alice and Bob use the Z basis, and Bob obtains a successful detection event (i.e., $y' \neq \varnothing$). As we are interested in the phase error rate defined in the single-photon emission events and all the statistics associated with the single-photons can be estimated using the decoy state method, in the virtual protocol we only consider the cases where Alice emits single photons.

To begin with, we first review briefly the main idea that we use to derive the phase error rate; it is based on the results introduced in [21], which follow the security analysis presented by Koashi in [26] based on a complementarity argument. This method [21] requires to estimate the transmission rates (i.e., detection probabilities) that Bob would obtain if he would measure some virtual states (see equation (78) below) in a complementary basis to the key generation basis. Importantly, it turns out that these transmission rates can be written as a liner combination of the transmission rates of the actual states sent by Alice (i.e., ρ_{0z}, ρ_{1z} and ρ_{0x}). To obtain these last transmission rates, we use the detection events that correspond to basis mismatch events (i.e., the detection events where Alice and Bob's basis choices are different). From these results, we can then calculate the exact value of the transmission rates associated to the virtual states (and, therefore, the phase error rate).

Based on this idea, we expand the security analysis introduced in [21] to accommodate the finite-key size effect in the following. For this, in the security proof we consider a virtual protocol that based on the complementarity argument [26] is equivalent to the actual protocol. In the virtual scheme, Alice prepares an ancilla qubit which is entangled with the pulse that she sends to Bob. Importantly, from Eve's viewpoint both protocols are completely indistinguishable because they emit the same quantum states and announce the same classical information.

In addition, as already mentioned in the main text, here we will consider the filtered states $\tilde{\rho}_{jz}$ and $\tilde{\rho}_{0x}$ only for convenience, as they allow us to simplify the mathematical derivation of the transmission rates associated to the virtual states. Note that due to the action of the filter operation we can concentrate only on those states that lie in the X–Z plane rather than in the whole Bloch sphere. Most importantly, we have that the relation derived for the filtered states holds as well for the actual states because all the states, which have the same σ_Y component, have the same probability of passing the filter. Indeed, one could obtain exactly the same mathematical expression for the main result of this section (see equation (103) below) without considering a filter operation, but the analysis is more cumbersome.

Let us start our analysis by introducing the following joint states, which we shall denote as $|\tilde{\psi}_{j_z}\rangle_{\mathrm{A_1,B}}$. They are a purification of the signals $\tilde{\rho}_{jz}$ with $j\in\{0,\ 1\}$ (see equation (32)),

$$\left|\tilde{\psi}_{j_z}\right\rangle_{\mathrm{A_1,B}} = \sqrt{P_0^{j_z}}\ |0\rangle_{\mathrm{A_1}}\left|\phi_0^{j_z}\right\rangle_{\mathrm{B}} + \sqrt{P_1^{j_z}}\ |1\rangle_{\mathrm{A_1}}\left|\phi_1^{j_z}\right\rangle_{\mathrm{B}}, \tag{75}$$

where the index $\mathrm{A_1}$ represents the ancilla system and the index B is the system that Alice sends to Bob. In addition, we define the state:

$$\left|\tilde{\Psi}_z\right\rangle_{\mathrm{A_1,A_2,B}} = \frac{1}{\sqrt{2}}\Big(|0\rangle_{\mathrm{A_2}}\left|\tilde{\psi}_{0_z}\right\rangle_{\mathrm{A_1,B}} + |1\rangle_{\mathrm{A_2}}\left|\tilde{\psi}_{1_z}\right\rangle_{\mathrm{A_1,B}}\Big), \tag{76}$$

where the ancilla system $\mathrm{A_2}$ stores the bit information. The aim of the virtual protocol is to quantify how accurately Bob can estimate Alice's measurement outcome if she would measure system $\mathrm{A_2}$ in the complementarity basis (i.e., if she would use the POVM $M_{X,\mathrm{A_2}} = \{|+\rangle\langle+|,\ |-\rangle\langle-|\}$, where $|\pm\rangle = 1/\sqrt{2}\,(|0\rangle \pm |1\rangle)$). This way one can characterize the information that Eve could have obtained about the raw key [26]. Note that equation (76) can be rewritten as

$$\begin{aligned}\left|\tilde{\Psi}_z\right\rangle_{\mathrm{A_1,A_2,B}} =& \sqrt{\frac{1+\langle\tilde{\psi}_{0_z}|\tilde{\psi}_{1_z}\rangle_{\mathrm{A_1,B}}}{2}}\ |+\rangle_{\mathrm{A_2}}\left|\tilde{\psi}_{0_x}^{\mathrm{vir}}\right\rangle_{\mathrm{A_1,B}}\\ &+\sqrt{\frac{1-\langle\tilde{\psi}_{0_z}|\tilde{\psi}_{1_z}\rangle_{\mathrm{A_1,B}}}{2}}\ |-\rangle_{\mathrm{A_2}}\left|\tilde{\psi}_{1_x}^{\mathrm{vir}}\right\rangle_{\mathrm{A_1,B}},\end{aligned} \tag{77}$$

where the normalized virtual states $|\tilde{\psi}_{j_x}^{\mathrm{vir}}\rangle_{\mathrm{A_1,B}}$, with $j\in\{0,\ 1\}$, are defined as

$$\left|\tilde{\psi}_{j_x}^{\mathrm{vir}}\right\rangle_{\mathrm{A_1,B}} = \frac{\left|\tilde{\psi}_{0_z}\right\rangle_{\mathrm{A_1,B}} + (-1)^j\left|\tilde{\psi}_{1_z}\right\rangle_{\mathrm{A_1,B}}}{\sqrt{2\left[1+(-1)^j\langle\tilde{\psi}_{0_z}|\tilde{\psi}_{1_z}\rangle_{\mathrm{A_1,B}}\right]}}. \tag{78}$$

Let us now introduce some additional notation before we describe in detail the different steps of the virtual protocol. In particular, the states prepared by Alice in the virtual protocol are given by

$$|\phi\rangle_{\mathrm{sh,A_1,B}} = \sum_{c=1}^{5}\sqrt{P(c)}\ |c\rangle_{\mathrm{sh}}\left|\phi^{(c)}\right\rangle_{\mathrm{A_1,B}}, \tag{79}$$

where the shield system sh belongs to Alice's laboratory, the states $|\phi^{(c)}\rangle_{\mathrm{A_1,B}}$ have the form

$$\begin{aligned}\left|\phi^{(1)}\right\rangle_{\mathrm{A_1,B}} &= \left|\tilde{\psi}_{0_x}^{\mathrm{vir}}\right\rangle_{\mathrm{A_1,B}},\\ \left|\phi^{(2)}\right\rangle_{\mathrm{A_1,B}} &= \left|\tilde{\psi}_{1_x}^{\mathrm{vir}}\right\rangle_{\mathrm{A_1,B}},\\ \left|\phi^{(3)}\right\rangle_{\mathrm{A_1,B}} &= \left|\tilde{\psi}_{0_z}\right\rangle_{\mathrm{A_1,B}},\\ \left|\phi^{(4)}\right\rangle_{\mathrm{A_1,B}} &= \left|\tilde{\psi}_{1_z}\right\rangle_{\mathrm{A_1,B}},\\ \left|\phi^{(5)}\right\rangle_{\mathrm{A_1,B}} &= \left|\tilde{\psi}_{0_x}\right\rangle_{\mathrm{A_1,B}},\end{aligned} \tag{80}$$

and the probabilities $P(c)$ are given by

$$\begin{aligned}P(1) &= \frac{p_z^2}{2}\Big(1+\left\langle\tilde{\psi}_{0_z}\middle|\tilde{\psi}_{1_z}\right\rangle_{\mathrm{A_1,B}}\Big),\\ P(2) &= \frac{p_z^2}{2}\Big(1-\left\langle\tilde{\psi}_{0_z}\middle|\tilde{\psi}_{1_z}\right\rangle_{\mathrm{A_1,B}}\Big),\\ P(3) &= P(4) = \frac{p_z p_x}{2},\\ P(5) &= p_x.\end{aligned} \tag{81}$$

Also, we define Bob's POVM for the Z and the X basis measurement as $M_{Z,\mathrm{B}} = \{M_{Z0}, M_{Z1}, M_{Z\mathrm{f}}\}$ and $M_{X,\mathrm{B}} = \{M_{X0}, M_{X1}, M_{X\mathrm{f}}\}$, respectively. Here, the operator $M_{Z(X)\mathrm{f}}$ corresponds to the inconclusive outcome in the Z (X) basis. Importantly, in the security analysis we assume that this operator is the same for both bases, i.e., $M_\mathrm{f} := M_{Z\mathrm{f}} = M_{X\mathrm{f}}$. Note that this assumption is met in all those actual experiments where the detection probability for any state is independent of Bob's basis choice, and this allows us to conceptually delay Bob's measurement basis choice until he is certain to obtain a conclusive result. That is, we consider that Bob first conducts a filter operation with Kraus operators $D = \{\sqrt{I - M_\mathrm{f}}, \sqrt{M_\mathrm{f}}\}$ followed by the Z or X basis measurement, which we redefine as $\{M_{Z0}, M_{Z1}\}$ and $\{M_{X0}, M_{X1}\}$, respectively.

Next we present the steps of the virtual protocol in detail.

Virtual protocol

Alice repeats the first step n_1 times, where n_1 is the number of single-photon emissions generated by Alice in the actual protocol within the set $|Z_{k_s}|$.

(1) *Preparation*

Alice prepares the state $|\phi\rangle_{\mathrm{sh,A_1,B}}$ given by equation (79). Afterwards, she sends Bob system B over a quantum channel and delays her measurement on system sh until step 3.

(2) *Filter operation*

Bob performs on system B the filter operation D and, if this operation succeeds, he stores this system in a quantum memory. We will denote the set of successful filter results as $\mathbf{S}$, and $|\mathbf{S}| = N_1$.

(3) *Collective measurement*

Alice and Bob perform on the states in the set $\mathbf{S}$ a collective measurement characterized by the POVM elements $F_{\Omega,s}$, with $\Omega \in \{1, 2, \ldots, 6\}$ and $s \in \{0, 1\}$ (see equation (84)) on the states in the set $\mathbf{S}$.

(4) *Classical communication*

Alice announces the Z (X) basis choice over an authenticated public channel when the result of her measurement in step 3 is $\Omega = 1, 2, 3, 4$ $(\Omega = 5, 6)$. Then, Bob announces the Z (X) basis choice, also over an authenticated public channel, when the measurement outcome in step 3 is $\Omega = 1, 2, 6$ $(\Omega = 3, 4, 5)$ to ensure that the classical information declared in both the actual and the virtual protocols coincide (see the main text below for further details). In addition, Bob declares the value of s when $\Omega = 3, 4, 5, 6$.

(5) *Estimation of the number of phase errors*

Alice and Bob calculate an upper bound on the number of phase errors. This upper bound is given by

$$N_{\mathrm{ph}}^{\mathrm{U}} = \overline{\Lambda_{1,1}^{(N_1)}} + \overline{\Lambda_{2,0}^{(N_1)}}, \tag{82}$$

where $\Lambda_{\Omega,s}^{(N_1)}$ denotes the number of outcomes associated to the operator $F_{\Omega,s}$ *after* N_1 trials, and $\overline{\Lambda_{\Omega,s}^{(N_1)}}$ is an upper bound on $\Lambda_{\Omega,s}^{(N_1)}$.

The size of the set $\mathbf{S}$ (see step 2 of the virtual protocol) is upper bounded by

$$|\mathbf{S}| = N_1 \leqslant \sum_{a,b\in\{Z,X\}} \sum_{y,y'\in\{0,1\}} \overline{\mathrm{Decoy}_1}(ay, by'), \tag{83}$$

where the parameter $\overline{\mathrm{Decoy}_1}(ay, by')$ is defined in appendix C. Also, the POVM elements $F_{\Omega,s}$ of Alice and Bob's collective measurement are given by

$$\begin{aligned} F_{\Omega,s} &= P\Big[|\Omega\rangle_{\mathrm{sh}}\Big] \otimes M_{Xs} \qquad \text{when} \Omega \in \{1, 2, 3, 4\}, \\ F_{5,s} &= P\Big[|5\rangle_{\mathrm{sh}}\Big] \otimes p_x M_{Xs}, \\ F_{6,s} &= P\Big[|5\rangle_{\mathrm{sh}}\Big] \otimes p_z M_{Zs}. \end{aligned} \tag{84}$$

These POVM elements satisfy $\sum_{s\in\{0,1\}} \sum_{\Omega\in\{1,\ldots,6\}} F_{\Omega,s} = I_{\mathrm{sh}} \otimes I_{\mathrm{B}}$.

It is easy to demonstrate that from Eve's viewpoint the virtual protocol described above is completely equivalent to the actual protocol. Indeed, the quantum states that Alice sends to Bob are exactly the same in both protocols. Also, both schemes declare precisely the same classical information. To see this last point, let us further clarify the fourth step of the virtual protocol. In particular, note that when $\Omega = 1(2)$ the state that Alice sends to Bob in the virtual protocol is $\mathrm{Tr}_{\mathrm{A_1}} P[|\tilde{\psi}_{0(1)x}\rangle_{\mathrm{A_1B}}]$ and Bob uses the X basis. However, in this case, Alice and Bob announce the Z basis. In so doing, the actual and virtual protocols are indistinguishable. This is so because in the actual protocol the events $\Omega = 1$ or 2 are used to generate a secret key, i.e., in these events both Alice and Bob select, and therefore also declare, the Z basis. Then, the virtual protocol has to do the same declaration, otherwise it could be distinguished from the actual protocol. That is, with our definition of the virtual protocol we guarantee that it produces precisely the same classical information as the actual protocol.

Next, we present the estimation method that we use in order to upper bound the quantities $\Lambda_{1,1}^{(N_1)}$ and $\Lambda_{2,0}^{(N_1)}$ using experimentally observed values. For this, we consider the sequence of random variables $X_{\Omega,s}^{(l)}$, with $l = 1, \ldots, N_1$, given by

$$X_{\Omega,s}^{(l)} = \Lambda_{\Omega,s}^{(l)} - \sum_{u=1}^{l} P_{\Omega,s}\left(u \middle| \xi_0, \ldots, \xi_{u-1}\right), \tag{85}$$

where $P_{\Omega,s}(u|\xi_0, \ldots, \xi_{u-1})$ is the conditional probability of obtaining the values Ω and s in the collective measurement performed in the u th trial of the third step of the virtual protocol, conditioned on the first $u - 1$ measurement outcomes from the collective measurements $\xi_0, \ldots, \xi_{u-1}$. To obtain this conditional probability we use the following joint state in N_1 trials

$$|\Phi\rangle_{\text{sh},\text{A}_1,\text{B}} = \left|\phi_{\overrightarrow{u-1}}\right\rangle_{\text{sh},\text{A}_1,\text{B}} \left|\phi_u\right\rangle_{\text{sh},\text{A}_1,\text{B}} \left|\phi_{\overrightarrow{N_1-u}}\right\rangle_{\text{sh},\text{A}_1,\text{B}}, \tag{86}$$

where $|\phi_{\overrightarrow{u-1}}\rangle_{\text{sh},\text{A}_1,\text{B}}$, $|\phi_u\rangle_{\text{sh},\text{A}_1,\text{B}}$, and $|\phi_{\overrightarrow{N_1-u}}\rangle_{\text{sh},\text{A}_1,\text{B}}$ represent, respectively, Alice's prepared states in the first $u - 1$ trials, in the u th trial, and in the rest of trials.

Let U_{BE} denote Eve's unitary transformation on Bob's system B and on her system E. We have that

$$U_{\text{BE}}\ |\Phi\rangle_{\text{sh},\text{A}_1,\text{B}} |0\rangle_{\text{E}} = \sum_t B_{t,\text{B}}\ |\Phi\rangle_{\text{sh},\text{A}_1,\text{B}} |t\rangle_{\text{E}}, \tag{87}$$

where $B_{t,\text{B}}$ denotes the Kraus operator which acts on system B depending on Eve's measurement outcome of her ancilla. Now we consider Alice and Bob's collective measurement. In particular, let M_{sh_v,s_v} represent the Kraus operator associated with the vth$(1 \leqslant v \leqslant u)$ measurement outcome of Alice's system sh and Bob's system. Also, let $\mathcal{O}_{u-1,\text{sh},\text{B}}$ denote Alice and Bob's joint measurement operator up to $u - 1$ trials. It can be written as

$$\mathcal{O}_{u-1,\text{sh},\text{B}} = \bigotimes_{v=1}^{u-1} M_{\text{sh}_v,s_v}\left(I_{\text{sh}} \otimes \sqrt{1 - M_{\text{f}}}\right). \tag{88}$$

We shall denote the measurement outcomes of the first $u - 1$ trials as O_{u-1}. Then, after Eve's intervention and conditioned on the fact of obtaining the measurement results O_{u-1}, we have that the normalized u th state of Alice's system sh and Bob's system B, which we shall represent as $\rho_{u|\overrightarrow{u-1}}^{\text{sh},\text{B}}$, is given by

$$\rho_{u|\overrightarrow{u-1}}^{\text{sh},\text{B}} = \frac{\sigma_{u|O_{u-1}}^{\text{sh},\text{B}}}{\text{Tr}\left(\sigma_{u|O_{u-1}}^{\text{sh},\text{B}}\right)}, \tag{89}$$

where the state $\sigma_{u|O_{u-1}}^{\text{sh},\text{B}}$ has the form

$$\sigma_{u|O_{u-1}}^{\text{sh},\text{B}} := \sum_t \text{Tr}_{\bar{u}}\left(P\left[\mathcal{O}_{u-1,\text{sh},\text{B}} B_{t,\text{B}}\ |\Phi\rangle_{\text{sh},\text{A}_1,\text{B}}\right]\right). \tag{90}$$

Here, $\text{Tr}_{\bar{u}}$ is the trace over all systems except for the u th systems sh and B. Equation (90) can be rewritten as follows:

$$\begin{aligned}\sigma_{u|O_{u-1}}^{\text{sh},\text{B}} &= \sum_t \sum_{\overrightarrow{u-1},\,\overrightarrow{N_1-u}} \text{Tr}_{\text{A}_1}^{(u)}\left(P\left[\left\langle\overrightarrow{u-1}\right|\left\langle\overrightarrow{N_1-u}\right|\mathcal{O}_{u-1,\text{sh},\text{B}} B_{t,\text{B}}\ \left|\phi_{\overrightarrow{u-1}}\right\rangle_{\text{sh},\text{A}_1,\text{B}}\left|\phi_u\right\rangle_{\text{sh},\text{A}_1,\text{B}}\left|\phi_{\overrightarrow{N_1-u}}\right\rangle_{\text{sh},\text{A}_1,\text{B}}\right]\right)\\ &= \sum_t \sum_{\overrightarrow{u-1},\,\overrightarrow{N_1-u}} \text{Tr}_{\text{A}_1}^{(u)}\left(P\left[A_{t,\text{B}|O_{u-1}}^{\overrightarrow{u-1},\,\overrightarrow{N_1-u}}\ \left|\phi_u\right\rangle_{\text{sh},\text{A}_1,\text{B}}\right]\right),\end{aligned} \tag{91}$$

where $\text{Tr}_{\text{A}_1}^{(u)}$ represents the trace over the $u$thA$_1$ system, the states $|\overrightarrow{u-1}\rangle$ and $|\overrightarrow{N_1-u}\rangle$ denote an orthogonal basis for the first $u - 1$ systems and the last $N_1 - u$ systems, respectively, and

$$A_{t,\text{B}|O_{u-1}}^{\overrightarrow{u-1},\overrightarrow{N_1-u}} := \left\langle\overrightarrow{u-1}\right|\left\langle\overrightarrow{N_1-u}\right|\mathcal{O}_{u-1,\text{sh},\text{B}} B_{t,\text{B}}\ \left|\phi_{\overrightarrow{u-1}}\right\rangle_{\text{sh},\text{A}_1,\text{B}}\left|\phi_{\overrightarrow{N_1-u}}\right\rangle_{\text{sh},\text{A}_1,\text{B}} \tag{92}$$

is the Kraus operator acting on the u th system conditioned on the measurement outcomes O_{u-1}.

Therefore, we obtain that the conditional probability defined in equation (85) for $\Omega \in \{1, \ldots, 6\}$ is given by

$$\begin{aligned} P_{\Omega,s}\left(u \middle| \xi_0, \ldots, \xi_{u-1}\right) &= \mathrm{Tr}\left\{ F_{\Omega,s} \frac{\mathcal{E}\left(\rho^{\mathrm{sh,B}}_{u\left|\overrightarrow{u-1}\right.}\right)}{\mathrm{Tr}\left[\mathcal{E}\left(\rho^{\mathrm{sh,B}}_{u\left|\overrightarrow{u-1}\right.}\right)\right]} \right\} \\ &= \frac{Q(\Omega)}{\mathrm{Tr}\left[\mathcal{E}\left(\rho^{\mathrm{sh,B}}_{u\left|\overrightarrow{u-1}\right.}\right)\right]\mathrm{Tr}\left(\sigma^{\mathrm{sh,B}}_{u|O_{u-1}}\right)} \mathrm{Tr}\left[\mathcal{M}_{Xs}^{\left(u\left|\overrightarrow{u-1}\right.\right)} \mathrm{Tr}_{\mathrm{A_1}} P\left[\left|\phi^{(\Omega)}\right\rangle_{\mathrm{A_1,B}}\right]\right] \\ &=: Q(\Omega)\, T_{M_{Xs}}^{\left(u\left|\overrightarrow{u-1}\right.\right)}\left[\mathrm{Tr}_{\mathrm{A_1}} P\left[\left|\phi^{(\Omega)}\right\rangle_{\mathrm{A_1,B}}\right]\right], \end{aligned} \tag{93}$$

where $\mathcal{E}(\rho) := (I_{\mathrm{sh}} \otimes \sqrt{I - M_{\mathrm{f}}})\rho(I_{\mathrm{sh}} \otimes \sqrt{I - M_{\mathrm{f}}})^{\dagger}$, the probability $Q(\Omega) = P(\Omega)$ for$\Omega \in \{1, 2, 3, 4\}$, $Q(5) = p_x P(5)$ and $Q(6) = p_z P(5)$, the operator $\mathcal{M}_{Xs}^{\left(u\left|\overrightarrow{u-1}\right.\right)} := \sum_t \sum_{\overrightarrow{u-1}, \overrightarrow{N_1-u}} (\sqrt{I - M_{\mathrm{f}}}\ A_{t,\mathrm{B}|O_{u-1}}^{\overrightarrow{u-1}, \overrightarrow{N_1-u}})^{\dagger} M_{Xs}(\sqrt{I - M_{\mathrm{f}}}\ A_{t,\mathrm{B}|O_{u-1}}^{\overrightarrow{u-1}, \overrightarrow{N_1-u}})$, the states $|\phi^{(\Omega)}\rangle_{\mathrm{A_1,B}}$ are defined in equation (80), and $T_{M_{Xs}}^{\left(u\left|\overrightarrow{u-1}\right.\right)}[\mathrm{Tr}_{A_1} P[|\phi^{(\Omega)}\rangle_{\mathrm{A_1,B}}]]$ is the u th conditional probability that Bob's measurement outcome in the X basis is $s \in \{0, 1\}$ given that Alice sends him the state $\mathrm{Tr}_{A_1} P[|\phi^{(\Omega)}\rangle_{\mathrm{A_1,B}}]$ and the filter operation succeeds conditioned on the first $u - 1$ measurement results. For convenience, we shall refer to $T_{M_{Xs}}^{\left(u\left|\overrightarrow{u-1}\right.\right)}[A]$ as the transmission rate of A.

If we apply Azuma's inequality (see *lemma 4* in appendix B), we obtain

$$\left| \sum_{u=1}^{N_1} P_{\Omega,s}\left(u \middle| \xi_0, \ldots, \xi_{u-1}\right) - \Lambda_{\Omega,s}^{(N_1)} \right| \leqslant \Delta_{\mathrm{A},\Omega}^{s}, \tag{94}$$

except with error probability $\epsilon_{\mathrm{A},\Omega}^{s}$, where $\Delta_{\mathrm{A},\Omega}^{s} = g_{\mathrm{A}}(N_1, \epsilon_{\mathrm{A},\Omega}^{s})$.

By combining this result with that from equation (93), we have that

$$\frac{\Lambda_{\Omega,s}^{(N_1)} - \Delta_{\mathrm{A},\Omega}^{s}}{Q(\Omega)} \leqslant \sum_{u=1}^{N_1} T_{M_{Xs}}^{\left(u\left|\overrightarrow{u-1}\right.\right)}\left[\mathrm{Tr}_{\mathrm{A_1}} P\left[\left|\phi^{(\Omega)}\right\rangle_{\mathrm{A_1,B}}\right]\right] \leqslant \frac{\Lambda_{\Omega,s}^{(N_1)} + \Delta_{\mathrm{A},\Omega}^{s}}{Q(\Omega)}. \tag{95}$$

Note that the parameters $\Lambda_{\Omega,s}^{(N_1)}$, with $\Omega \in \{3, 4, 5\}$, can be upper and lower bounded using the decoy-state method. We shall denote the failure probability of this estimation as $\epsilon_{Z0,Xs}$, $\epsilon_{Z1,Xs}$ and $\epsilon_{X0,Xs}$, respectively.

As a result, we obtain bounds on $\sum_{u=1}^{N_1} T_{M_{Xs}}^{\left(u\left|\overrightarrow{u-1}\right.\right)}[\mathrm{Tr}_{A_1} P[|\phi^{(\Omega)}\rangle_{\mathrm{A_1,B}}]]$ that maximize the number of phase errors N_{ph} in the single-photon emissions within the set $|Z_{k_s}|$. They are denoted as $N_{M_{Xs}}(\Omega)$ and have the form

$$N_{M_{Xs}}(3) := \left\{ \frac{\underline{\underline{\mathrm{Decoy}_1}}(Z0, Xs) - \Delta_{\mathrm{A},3}^{s}}{Q(3)} \text{ or } \frac{\overline{\mathrm{Decoy}_1}(Z0, Xs) + \Delta_{\mathrm{A},3}^{s}}{Q(3)} \right\}, \tag{96}$$

$$N_{M_{Xs}}(4) := \left\{ \frac{\underline{\underline{\mathrm{Decoy}_1}}(Z1, Xs) - \Delta_{\mathrm{A},4}^{s}}{Q(4)} \text{ or } \frac{\overline{\mathrm{Decoy}_1}(Z1, Xs) + \Delta_{\mathrm{A},4}^{s}}{Q(4)} \right\}, \tag{97}$$

$$N_{M_{Xs}}(5) := \left\{ \frac{\underline{\underline{\mathrm{Decoy}_1}}(X0, Xs) - \Delta_{\mathrm{A},5}^{s}}{Q(5)} \text{ or } \frac{\overline{\mathrm{Decoy}_1}(X0, Xs) + \Delta_{\mathrm{A},5}^{s}}{Q(5)} \right\}. \tag{98}$$

When $\Omega \in \{1, 2\}$, the quantity $T_{M_{Xs\oplus 1}}^{\left(u\left|\overrightarrow{u-1}\right.\right)}\left[\tilde{\rho}_{sx}^{\mathrm{vir}}\right]$, with $s \in \{0, 1\}$, represents the transmission rate of the virtual states $\tilde{\rho}_{sx}^{\mathrm{vir}} = \mathrm{Tr}_B(P[|\tilde{\psi}_{s_x}^{\mathrm{vir}}\rangle_{\mathrm{A_1,B}}])$, with $|\tilde{\psi}_{s_x}^{\mathrm{vir}}\rangle_{\mathrm{A_1,B}}$ given by equation (78). This quantity can be decomposed into the transmission rate of the Pauli operators σ_I, σ_X and σ_Z. However, for later convenience, we will decompose it as a function of $\tilde{\rho}_{0z}$ and $\tilde{\rho}_{1z}$, together with σ_I, σ_X and σ_Z. Here, the states $\tilde{\rho}_{0_z}$ and $\tilde{\rho}_{1_z}$ are defined in equation (31). In particular, from equation (78) we find that

$$\begin{aligned}
T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{sx}^{\mathrm{vir}}\right] &= \frac{1}{2\left[1+(-1)^s\left\langle\tilde{\psi}_{0_z}\middle|\tilde{\psi}_{1_z}\right\rangle_{\mathrm{A_1,B}}\right]}\left\{T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{0z}\right]+T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{1z}\right]\right.\\
&\quad+(-1)^s\left(T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\mathrm{Tr}_B\left(P\left[\left|\tilde{\psi}_{0_z}\right\rangle\left\langle\tilde{\psi}_{1_z}\right|_{\mathrm{A_1,B}}\right]\right)\right]\right.\\
&\quad\left.\left.+T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\mathrm{Tr}_B\left(P\left[\left|\tilde{\psi}_{1_z}\right\rangle\left\langle\tilde{\psi}_{0_z}\right|_{\mathrm{A_1,B}}\right]\right)\right]\right)\right\}\\
&= \frac{1}{2\left\{1+(-1)^s\left(\sqrt{P_0^{0z}P_0^{1z}}\left\langle\phi_0^{0z}\middle|\phi_0^{1z}\right\rangle+\sqrt{P_1^{0z}P_1^{1z}}\left\langle\phi_1^{0z}\middle|\phi_1^{1z}\right\rangle\right)\right\}}\\
&\quad\left[T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{0z}\right]+T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{1z}\right]\right.\\
&\quad+(-1)^s\sum_{t=0}^{1}\sqrt{P_t^{0z}P_t^{1z}}\left\{\left(a_t^{0z}a_t^{1z}+b_t^{0z}b_t^{1z}\right)T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_I\right]\right.\\
&\quad+\left(a_t^{0z}b_t^{1z}+a_t^{0z}b_t^{1z}\right)T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_X\right]\\
&\quad\left.\left.+\left(a_t^{0z}a_t^{1z}-b_t^{0z}b_t^{1z}\right)T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_Z\right]\right\}\right],
\end{aligned}\qquad(99)$$

where we have used equation (75) in the second equality and see equation (35) for the definition of a_t^S and b_t^S.

In addition, we have that the transmission rate of $\tilde{\rho}_{0z}$, $\tilde{\rho}_{1z}$ and $\tilde{\rho}_{0x}$ can be decomposed using the Pauli operators as follows

$$\begin{aligned}
&\begin{pmatrix} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{0z}\right]\\ T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{1z}\right]\\ T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{0x}\right]\end{pmatrix}\\
&=\begin{pmatrix}1/2 & r_x^{0z}/2 & r_z^{0z}/2\\ 1/2 & r_x^{1z}/2 & r_z^{1z}/2\\ 1/2 & r_x^{0x}/2 & r_z^{0x}/2\end{pmatrix}\begin{pmatrix} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_I\right]\\ T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_X\right]\\ T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_Z\right]\end{pmatrix}=:A\begin{pmatrix} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_I\right]\\ T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_X\right]\\ T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_Z\right]\end{pmatrix}.
\end{aligned}\qquad(100)$$

Hence, the transmission rate of the Pauli operators can be described as

$$\begin{pmatrix} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_I\right]\\ T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_X\right]\\ T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\sigma_Z\right]\end{pmatrix}=A^{-1}\begin{pmatrix} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{0z}\right]\\ T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{1z}\right]\\ T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{0x}\right]\end{pmatrix},\qquad(101)$$

where the inverse matrix A^{-1} is given in equation (37).

Now, if we combine equations (99), (101) and (95), we obtain that $N_{\rm ph}$ is upper bounded by

$$\begin{aligned} N_{\rm ph} = \Lambda_{1,1}^{(N_1)} + \Lambda_{2,0}^{(N_1)} &\leqslant \sum_{s=0}^{1} P(s+1) \sum_{u=1}^{N_1} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{sx}^{\rm vir}\right] + \Delta_{{\rm A},s+1}^{s\oplus 1} \\ &= \sum_{s=0}^{1} \frac{P(s+1)}{2\left\{1+(-1)^s\left(\sqrt{P_0^{0z}P_0^{1z}}\left\langle\phi_0^{0z}\middle|\phi_0^{1z}\right\rangle + \sqrt{P_1^{0z}P_1^{1z}}\left\langle\phi_1^{0z}\middle|\phi_1^{1z}\right\rangle\right)\right\}} \\ &\quad \left[\sum_{u=1}^{N_1} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{0z}\right] + \sum_{u=1}^{N_1} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{1z}\right]\right. \\ &\quad + (-1)^s \sum_{t=0}^{1} \sqrt{P_t^{0z}P_t^{1z}}\left\{C_{t,0}\sum_{u=1}^{N_1} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{0z}\right] + C_{t,1}\sum_{u=1}^{N_1} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{1z}\right]\right. \\ &\quad \left.\left. + C_{t,2}\sum_{u=1}^{N_1} T_{M_{Xs\oplus 1}}^{\left(u\middle|\overrightarrow{u-1}\right)}\left[\tilde{\rho}_{0x}\right]\right\}\right] + \Delta_{{\rm A},s+1}^{s\oplus 1}. \end{aligned} \tag{102}$$

Finally, by using the results given by equations (96)–(98), we find that

$$\begin{aligned} N_{\rm ph} \leqslant \sum_{s=0}^{1} &\frac{P(s+1)}{2\left\{1+(-1)^s\left(\sqrt{P_0^{0z}P_0^{1z}}\left\langle\phi_0^{0z}\middle|\phi_0^{1z}\right\rangle + \sqrt{P_1^{0z}P_1^{1z}}\left\langle\phi_1^{0z}\middle|\phi_1^{1z}\right\rangle\right)\right\}}\left[N_{M_{Xs}}(3) + N_{M_{Xs}}(4)\right. \\ &\left. + (-1)^s\sum_{t=0}^{1}\sqrt{P_t^{0z}P_t^{1z}}\left\{C_{t,0}N_{M_{Xs}}(3) + C_{t,1}N_{M_{Xs}}(4) + C_{t,2}N_{M_{Xs}}(5)\right\}\right] + \Delta_{{\rm A},s+1}^{s\oplus 1} \end{aligned} \tag{103}$$

$$=: N_{\rm ph}^{\rm U}, \tag{104}$$

except with error probability

$$\begin{aligned} \varepsilon_{\rm ph} = \epsilon_{{\rm A},1}^{1} + \epsilon_{{\rm A},2}^{0} + \sum_{s\in\{0,1\},\Omega\in\{3,4,5\}} \epsilon_{{\rm A},\Omega}^{s} \\ + \sum_{s\in\{0,1\}}\left(\epsilon_{Z0,Xs} + \epsilon_{Z1,Xs} + \epsilon_{X0,Xs}\right), \end{aligned} \tag{105}$$

where $\epsilon_{{\rm A},\Omega}^{s}$ is the failure probability that equation (94) does not hold for $\Omega\in\{1,\ldots,5\}$ and $s\in\{0,1\}$. Also, $\epsilon_{Z0(1),Xs}$ and $\epsilon_{X0,Xs}$ are the failure probabilities of the decoy state method i.e., the failure probabilities of the estimation of $\Lambda_{3(4),s}^{(N_1)}$ and $\Lambda_{5,s}^{(N_1)}$, respectively.

Appendix E. Simulation

In this appendix we present the calculations used to obtain figures 2, 4 and 6 in the main text.

In particular, we consider that Alice sends Bob pairs of coherent states of the form $|\sqrt{k_{\rm ref}}\,{\rm e}^{{\rm i}\chi}\rangle_{\rm r}|\sqrt{k_{\rm sig}}\,{\rm e}^{{\rm i}(\chi+\theta_{\rm A}+\Delta\theta_{\rm A})}\rangle_{\rm s}$, and we set Alice's (Bob's) phase modulation error to $\Delta\theta_{\rm A} = \xi\theta_{\rm A}/\pi$ ($\Delta_{\rm B} = -\Delta_{\rm A}$). Also, we assume a Gaussian distribution for the intensity fluctuations of the laser within an interval $[k^-, k^+]$. That is, we consider that the probability density function of the fluctuations is given by $p_{\rm G}(k) = A\exp[-(k-\mu)^2/2\sigma^2]$, where μ is the desired value (e.g., $k_{\rm s}$, $k_{\rm d1}$, and $k_{\rm d2}$), the dispersion σ^2 has the form $\sigma^2 = r\mu/5$, and the normalization factor A is such that $\int_{k^-}^{k^+} p_{\rm G}(k){\rm d}k = 1$.

Calculation of the parameters $m_0^{\rm L}$ and $m_1^{\rm L}$.

For this, we need to obtain $|Z_k|$ for all $k\in K$. Afterwards, we simply apply the procedure described in section 4.1 (for the exact intensity control case) and in section 4.2 (for the intensity fluctuation case).

We consider that the total number of pulses sent by Alice using the intensity setting k is given by $N_k = Np_k$, where N denotes the total number of transmissions until the conditions in the Sifting step of the protocol are met. The total system loss $\eta_{\rm sy} := \eta_{\rm det}\,\eta_{\rm ch}$ includes the channel loss and the detection efficiency of Bob's detectors. The conditional probability $p^{(k)}(Zj|Zi)$ that Bob obtains the bit $j\in\{0,1\}$ using the Z basis given that Alice sends him a bit i encoded with the intensity k and also in the Z basis can be written as

$$p^{(k)}(Z0|Z0) = \int_{k^-}^{k^+} p_{\rm G}(k)\left[1-\left(1-p_{\rm d}\right){\rm e}^{-\eta_{\rm sy}k}\right]{\rm d}k, \tag{106}$$

$$p^{(k)}(Z1|Z0) = p_{\rm d}, \tag{107}$$

$$p^{(k)}(Zj|Z1) = \int_{k^-}^{k^+} p_{\mathrm{G}}(k)\left[1 - \left(1 - p_{\mathrm{d}}\right)\exp\left(-\frac{\eta_{\mathrm{sy}}k\left(1-(-1)^j\cos\xi\right)}{2}\right)\right]\mathrm{d}k. \tag{108}$$

The conditional probability $p^{(k)}(Zj \wedge \overline{Zj\oplus 1}|Zi)$ that Bob interprets the bit value j (after a random assignment of double click events to single clicks events) when he uses the Z basis given that Alice sends him a pulse with the intensity k, prepared in the Z basis, and encoding the bit value i is written as

$$\begin{aligned} p^{(k)}\left(Zj \wedge \overline{Zj\oplus 1}\middle|Zi\right) = {} & p^{(k)}(Zj|Zi)\left(1 - p^{(k)}(Zj\oplus 1|Zi)\right) \\ & + \frac{1}{2}p^{(k)}(Zj|Zi)p^{(k)}(Zj\oplus 1|Zi). \end{aligned} \tag{109}$$

To simulate the misalignment in the optical system we transform this probability as

$$P^{(k)}\left(Zj \wedge \overline{Zj\oplus 1}\middle|Zj\right) = p^{(k)}\left(Zj \wedge \overline{Zj\oplus 1}\middle|Zj\right)\left(1 - e_{\mathrm{mis}}\right), \tag{110}$$

$$P^{(k)}\left(Zj\oplus 1 \wedge \overline{Zj}\middle|Zj\right) = p^{(k)}\left(Zj \wedge \overline{Zj\oplus 1}\middle|Zj\right)e_{\mathrm{mis}} + p^{(k)}\left(Zj\oplus 1 \wedge \overline{Zj}\middle|Zj\right). \tag{111}$$

In so doing, we obtain

$$|Z_k| = N_k p_z^2 \sum_{i,j\in\{0,1\}} P^{(k)}\left(Zj \wedge \overline{Zj\oplus 1}\middle|Zi\right). \tag{112}$$

The bit error rate in the Z basis when Alice sends Bob a pulse using the signal intensity is given by

$$e_z = \frac{\sum_{j\in\{0,1\}} P^{(k_s)}\left(Zj\oplus 1 \wedge \overline{Zj}\middle|Zj\right)}{\sum_{i,j\in\{0,1\}} P^{(k_s)}\left(Zj \wedge \overline{Zj\oplus 1}\middle|Zi\right)}. \tag{113}$$

Calculation of the parameter N_{ph}.

According to equation (36), we have that N_{ph} is upper bounded by

$$\begin{aligned} N_{\mathrm{ph}} \leqslant {} & \frac{1-\sin\frac{\xi}{2}}{2}\left(\frac{p_z}{p_x}\right)^2\left(\overline{\mathrm{Decoy}}_1(X0, X1) + \Delta^1_{\mathrm{A},5}\right) \\ & + \frac{p_z}{p_x}\left(\overline{\mathrm{Decoy}}_1(Z0, X0) + \overline{\mathrm{Decoy}}_1(Z1, X0) + \Delta^0_{\mathrm{A},3} + \Delta^0_{\mathrm{A},4}\right) \\ & - \frac{1-\sin\frac{\xi}{2}}{2}\left(\frac{p_z}{p_x}\right)^2\left(\underline{\mathrm{Decoy}}_1(X0, X0) + \Delta^0_{\mathrm{A},5}\right) + \Delta_{\mathrm{A},1} + \Delta_{\mathrm{A},2}. \end{aligned} \tag{114}$$

To obtain $\overline{\mathrm{Decoy}}_1(X0, X1)$ and $\underline{\mathrm{Decoy}}_1(X0, X0)$ we first calculate the probability $p^{(k)}(Xj \wedge \overline{Xj\oplus 1}|X0)$ that Bob obtains the bit j with the X basis given that Alice sends him a pulse of intensity k using the X basis and encoding the bit value 0. For this, we have that

$$p^{(k)}(Xj|X0) = \int_{k^-}^{k^+} p_{\mathrm{G}}(k)\left[1 - \exp\left[-\frac{\eta_{\mathrm{sy}}k\left(1+(-1)^j\cos\xi\right)}{2}\right]\left(1 - p_{\mathrm{d}}\right)\right]\mathrm{d}k. \tag{115}$$

Then, by using equation (109) we find

$$\begin{aligned} p^{(k)}\left(Xj \wedge \overline{Xj\oplus 1}\middle|X0\right) = {} & p^{(k)}(Xj|X0)\left(1 - p^{(k)}(Xj\oplus 1|X0)\right) \\ & + \frac{1}{2}p^{(k)}(X0|X0)p^{(k)}(X1|X0). \end{aligned} \tag{116}$$

Finally, we include the effect of the misalignment in the optical systems. That is, we transform $p^{(k)}(Xj \wedge \overline{Xj\oplus 1}|Xi)$ as

$$P^{(k)}\left(X0 \wedge \overline{X1}\middle|X0\right) = p^{(k)}\left(X0 \wedge \overline{X1}\middle|X0\right)\left(1 - e_{\mathrm{mis}}\right), \tag{117}$$

$$P^{(k)}\left(X1 \wedge \overline{X0}\middle|X0\right) = p^{(k)}\left(X0 \wedge \overline{X1}\middle|X0\right)e_{\mathrm{mis}} + p^{(k)}\left(X1 \wedge \overline{X0}\middle|X0\right). \tag{118}$$

The number $|X_k^j|$ is therefore given by

$$|X_k^j| = N_k p_x^2 P^{(k)}\left(Xj \wedge \overline{Xj\oplus 1}\middle|X0\right). \tag{119}$$

Next, we calculate $\overline{\mathrm{Decoy}}_1(Z0, X0)$ and $\overline{\mathrm{Decoy}}_1(Z1, X0)$. For this we need to obtain $|Z^iX_k^j|$. We have that the probability $p^{(k)}(Xj|Zi)$ that Bob obtains the bit j with the X basis given that Alice sends him a pulse of intensity k, prepared in the Z basis, and encoding the bit value i is given by

$$p^{(k)}(Xj|Z0) = \int_{k^-}^{k^+} p_{\rm G}(k)\left[1 - \exp\left(\frac{-\eta_{\rm sy}k\left(1 + (-1)^j \sin \xi/2\right)}{2}\right)\left(1 - p_{\rm d}\right)\right]{\rm d}k, \tag{120}$$

$$p^{(k)}(Xj|Z1) = \int_{k^-}^{k^+} p_{\rm G}(k)\left[1 - \exp\left(\frac{-\eta_{\rm sy}k\left(1 - (-1)^j \sin 3\xi/2\right)}{2}\right)\left(1 - p_{\rm d}\right)\right]{\rm d}k. \tag{121}$$

In this scenario the probability $P^{(k)}(Xj \ \wedge \ \overline{Xj \oplus 1}|Zi)$ has the form

$$P^{(k)}\left(Xj \ \wedge \ \overline{Xj \oplus 1}\middle|Zi\right) = p^{(k)}(Xj|Zi)\left(1 - p^{(k)}(Xj \oplus 1|Zi)\right) + \frac{1}{2}p^{(k)}(Xj|Zi)p^{(k)}(Xj \oplus 1|Zi), \tag{122}$$

and therefore the quantity $|Z^i X_k^j|$ can be written as

$$|Z^i X_k^j| = N_k \frac{p_x p_z}{2} P^{(k)}\left(Xj \ \wedge \ \overline{Xj \oplus 1}\middle|Zi\right). \tag{123}$$

References

[1] Gisin N, Ribordy R, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95

[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[3] Lo H K, Curty M and Tamaki K 2014 *Nat. Photonics* **8** 595–604

[4] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev.* A **78** 042333
Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photonics* **4** 686
Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev. Lett.* **107** 110501
Weier H, Krauss H, Rau M, Fürst M, Nauerth S and Weinfurter H 2011 *New J. Phys.* **13** 073024
Jouguet P, Kunz-Jacques S and Diamanti E 2013 *Phys. Rev.* A **87** 062313
Bugge A N, Sauge S, Ghazali A M M, Skaar J, Lydersen L and Makarov V 2014 *Phys. Rev. Lett.* **112** 070503

[5] Lim C C W, Walenta N, Legré M, Gisin N and Zbinden H 2015 *IEEE J. Sel. Top. Quantum Electron.* **21** 3

[6] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634

[7] Hayashi M and Tsurumaru T 2012 *New J. Phys.* **14** 093014

[8] Lim C C W, Curty M, Walenta N, Xu F and Zbinden H 2014 *Phys. Rev.* A **89** 022307

[9] Hayashi M and Nakayama R 2014 *New J. Phys.* **16** 063009

[10] Korzh B, Lim C C W, Houlmann R, Gisin N, Li M J, Nolan D, Sanguinetti B, Thew R and Zbinden H 2015 *Nat. Photonics* **9** 163–8

[11] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503

[12] Ma X, Fung C-H F and Razavi M 2012 *Phys. Rev.* A **86** 052305
Wang X-B 2013 *Phys. Rev.* A **87** 012320
Xu F, Curty M, Qi B and Lo H K 2013 *New J. Phys.* **15** 113007
Mizutani A, Tamaki K, Ikuta R, Yamamoto T and Imoto N 2014 *Sci. Rep.* **4** 5236
Azuma K, Tamaki K and Munro W-J 2014 arXiv:1408.2884

[13] Curty M, Xu F, Cui W, Lim C C W, Tamki K and Lo H K 2014 *Nat. Commun.* **5** 3732

[14] Li Z, Zhang Y C, Xu F, Peng X and Guo H 2014 *Phys. Rev.* A **89** 052301
Ottaviani C, Spedalieri G, Braunstein S L and Pirandola S 2015 *Phys. Rev.* A **91** 022320
Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 *Nat. Photonics* **9** 397–402
Xu F, Curty M, Qi B, Qian L and Lo H-K 2015 arXiv:1506.04819
Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 arXiv:1506.06748

[15] da Silva F T, Vitoreti D, Xavier G B, do Amaral G C, Temporão G P and von der Weid J P 2013 *Phys. Rev.* A **88** 052303
Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
Liu Y *et al* 2013 *Phys. Rev. Lett.* **111** 130502
Xu F, Qi B, Liao Z and Lo H K 2013 *Appl. Phys. Lett.* **103** 061101
Tang Z, Liao Z, Xu F, Qi B, Qian L and Lo H K 2014 *Phys. Rev. Lett.* **112** 190503

[16] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[17] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[18] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[19] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **5** 325

[20] Lo H K and Preskill J 2007 *Quantum Inf. Comput.* **8** 431–58
Tamaki K, Lo H K, Fung C-H F and Qi B 2012 *Phys. Rev.* A **85** 042307

[21] Tamaki K, Curty M, Kato G, Lo H K and Azuma K 2014 *Phys. Rev.* A **90** 052314

[22] Bennett C H and Brassard G *Proc. Int. Conf. on Computers, Systems and Signal Processing* (Piscataway, NJ: IEEE) pp 175–9

[23] Mayers D 1996 *Advances in Cryptology-Proc. Crypto'96* (Springer: Berlin) p 343

[24] Lo H K and Chau H F 1999 *Science* **283** 2050

[25] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[26] Koashi M 2009 *New J. Phys.* **11** 045018

[27] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501

[28] Xu F, Sajeed S, Kaiser S, Tang Z, Qian L, Makarov V and Lo H K 2014 arXiv:1408.3667

[29] Wang X B, Peng C Z, Zhang J, Yang L and Pan J W 2008 *Phys. Rev.* A **77** 042311
Zhao Y, Qi B and Lo H K 2008 *Phys. Rev.* A **77** 052327
Peng X, Jiang H, Xu B J, Ma X and Guo H 2008 *Opt. Lett.* **33** 2077
Zhao Y, Qi B, Lo H K and Qian L 2010 *New J. Phys.* **12** 023024
Peng X, Xu B J and Guo H 2010 *Phys. Rev.* A **81** 042320
Hu J Z and Wang X B 2010 *Phys. Rev.* A **82** 012331

[30] Ben-Or M, Horodecki M, Leung D W, Mayers D and Oppenheim J 2005 *Theory of Cryptography: Second Theory of Cryptography Conf. TCC 2005* (*Lecture Notes in Computer Science* vol 3378) ed J Kilian (Berlin: Springer) pp 386–406
Müller-Quade J and Renner R 2009 *New J. Phys.* **11** 085006

[31] Cao Z, Zhang Z, Lo H K and Ma X 2015 *New J. Phys.* **17** 053014

[32] Koashi M 2005 arXiv: quant-ph/0505108

[33] Koashi M 2007 arXiv:0704.3661

[34] Chernoff H 1952 *Ann. Math. Sat.* **23** 493–507

[35] Hoeffding W 1963 *J. Am. Stat. Assoc.* **58** 13–30

[36] Azuma K 1967 *Tohoku Math. J.* **19** 357

[37] Boileau J C, Tamaki K, Batuwantudawe J, Laflamme R and Renes J M 2005 *Phys. Rev. Lett.* **94** 040503
Tamaki K, Lütkenhaus N, Koashi M and Batuwantudawe J 2009 *Phys. Rev.* A **80** 032302