IOP Publishing Quantum Sci. Technol. 10 (2025) 035002 https://doi.org/10.1088/2058-9565/adc8cc

Quantum Science and Technology

OPEN ACCESS

RECEIVED
18 January 2025

REVISED
7 March 2025

ACCEPTED FOR PUBLICATION
3 April 2025

PUBLISHED
22 April 2025

PAPER

Loss-tolerant quantum key distribution with detection efficiency mismatch

Alessandro Marcomini[1,2,3,*], **Akihiro Mizutani**[4], **Fadri Grünenfelder**[1,2,3], **Marcos Curty**[1,2,3] and **Kiyoshi Tamaki**[4]

[1] Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain
[2] Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
[3] AtlanTTic Research Center, University of Vigo, Vigo E-36310, Spain
[4] Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan
[*] Author to whom any correspondence should be addressed.

E-mail: amarcomini@vqcc.uvigo.es

Keywords: QKD, quantum communications, quantum cryptography, loss-tolerant QKD, detection efficiency mismatch

Abstract

Current implementations of quantum key distribution (QKD) typically rely on prepare-and-measure (P&M) schemes. Unfortunately, these implementations are not completely secure, unless security proofs fully incorporate all imperfections of real devices. So far, existing proofs have primarily focused on imperfections of either the light source or the measurement device. In this paper, we establish a security proof for the loss-tolerant P&M QKD protocol that incorporates imperfections in both the source and the detectors. Specifically, we demonstrate the security of this scheme when the emitted states deviate from the ideal ones and Bob's measurement device does not meet the basis-independent detection efficiency condition. Furthermore, we conduct an experiment to characterise the detection efficiency mismatch of commercial single-photon detectors as a function of the polarisation state of the input light, and determine the expected secret key rate in the presence of state preparation flaws when using such detectors. Our work provides a way towards guaranteeing the security of actual implementations of widely deployed P&M QKD.

1. Introduction

Quantum key distribution (QKD) offers the potential for communication certified with information-theoretic security by utilizing the principles of quantum mechanics. Specifically, it enables two legitimate parties, Alice and Bob, to generate a shared symmetric secret key, regardless of any eavesdropping effort by a third party (Eve) [1–3].

As of today, significant results have been achieved to show how QKD can be deployed both in metropolitan and inter-city networks [4–7] and over ground-to-satellite links [7, 8], as well as in commercial systems [9–11]. Still, the widespread of this technology is challenged by the fact that real-world devices present imperfections, potentially implying unnoticed security loopholes or information leakages. This fact is remarked by the richness of literature in the field of quantum hacking [12–14], by examples of successful attacks [15–20] and continuously proposed malicious schemes [21–26]. As a consequence, introducing security proofs for QKD with realistic devices has become of paramount importance [27].

The most vulnerable part of a QKD setup is widely acknowledged to be the receiver, as it welcomes all signals coming from the quantum channel. As a consequence, Eve can send additional light to the detectors, inducing information leakage (e.g. through the so-called Trojan-horse attack [28, 29]), forcing a convenient operational regime of the detectors (e.g. via an after-gate attack for gated detectors [30]) or directly blinding them using bright light [16, 17]. Moreover, even if the aforementioned attacks could be prevented [31, 32], the response of single-photon detectors (SPDs) typically depends on several degrees of freedom, such as time of arrival, frequency, polarisation and spatial modes of the incoming pulses [33–36]. This allows Eve to

manipulate the detection probability of the SPDs by changing the properties of the arriving signals [15, 19]. As QKD protocols require to discriminate different states at the receiver, multiple SPDs are usually needed. Since realistic devices cannot be identical, Eve might modify the incoming quantum states in such a way that a specific outcome detection is highly favoured. The latter issue is commonly addressed as detection efficiency mismatch (DEM) [37–43].

On the transmitter side, security threats are typically less concerning. For example, issues related to multi-photon emissions can be mitigated by means of the decoy-state method [44–48], while the effect of state preparation flaws (SPFs) has been shown to be almost negligible thanks to the so-called loss-tolerant (LT) approach [49] (although the latter crucially requires identical detectors). The effect of side-channels has also been intensively studied [50–56].

As a result, in the last decade huge effort has been dedicated to the design of QKD protocols based on quantum interference that could lift all assumptions on the receiver side, namely measurement-device-independent [57] and twin-field QKD [58]. While on-field realisations of these schemes have been achieved over large distances [59–61], prepare-and-measure (P&M) protocols are still being preferred for short- and mid-range communication and for industrial products due to their simpler implementation. Thus, the development of security proofs that can jointly account for both transmitter and receiver imperfections is of great relevance.

In this work we extend the security proof for LT QKD to accommodate the existence of a DEM. In doing so, we provide a unique recipe to establish the asymptotic security of P&M QKD protocols against coherent attacks in the presence of both SPFs and DEM. Moreover, we conduct an experiment to characterise the DEM in commercial SPDs and show that a secret key can be generated using such devices, even in the presence of large SPFs. In detail, we adopt the complementarity framework introduced by Koashi [62] to provide an upper bound on the phase-error rate, which ultimately quantifies the amount of privacy amplification that Alice and Bob must perform in the postprocessing phase of the QKD protocol. Our idea generalises the LT approach to the case in which the detection probability associated to the two measurement bases differs. In particular, we show that characterising the efficiency of the SPDs and monitoring the send-and-receive statistics of the protocol is enough to directly estimate all quantities involved in the computation of the secret key rate (SKR). In so doing, we generalise and simplify the technique developed in [37].

The paper is organised as follows. In section 2 we illustrate the underlying assumptions for our analysis, while in section 3 we present the details of the QKD scheme we evaluate. In section 4 we report the main results of our study and provide a full procedure for the estimation of the SKR. We show the applicability of our analysis by performing an experimental characterisation of two real detectors and studying how the DEM affects performance in section 5. Finally, we discuss the implications of our work in section 6 and conclude with some remarks in section 7. Further calculations and discussions can be found in the Appendices.

2. Assumptions

Our analysis relies on the following assumptions, whose implications are further discussed in appendix A.

(A1) Alice has a perfect single-photon source and she knows the qubit states $\{|\phi_i\rangle_B\}_i$, with $i \in \{0_Z, 1_Z, 0_X\}$, that she is sending to Bob. These might be different from the perfect $|i\rangle_B$ states (i.e. the eigenstates of the $\hat{Z}$ and $\hat{X}$ Pauli matrices). Moreover, we assume the flawed states $\{|\phi_i\rangle_B\}_i$ to be pairwise linearly independent and to lay on the $XZ-$plane of the Bloch sphere (which is always true, up to a lifting filtering operation, as discussed in appendix A.2).

(A2) Alice's lab is perfectly shielded from the eavesdropper such that no unwanted information leakage occurs (i.e. there is no side channel in Alice's source).

(A3) Bob employs an active BB84 receiver with two detectors. This means that the detectors are placed after a basis selector such that the detector D_0 (D_1) measuring 0_Z (1_Z) is also employed to measure 0_X (1_X).

(A4) Bob receives the system B in a qubit space.

(A5) As illustrated in appendix A.2, Bob's positive operator-valued measure (POVM) element assigning outcome $s \in \{0,1\}$ in the basis $\beta \in \{X,Z\}$ has the form

$$\hat{M}_{BT}^{s_\beta} = |s_\beta\rangle\langle s_\beta|_B \otimes \left(\hat{F}_s^{\dagger}\hat{F}_s\right)_T, \tag{1}$$

while the POVM element associated to a failed detection in the basis β is given by

$$\hat{M}_{BT}^{\text{fail}_\beta} = \hat{\mathbb{1}} - \hat{M}_{BT}^{0_\beta} - \hat{M}_{BT}^{1_\beta}. \tag{2}$$

Here, T denotes an additional system of arbitrary dimension corresponding to a given efficiency-affecting mode (e.g. time of arrival, frequency, polarisation or spatial mode), while $\hat{F}_s^{\dagger}\hat{F}_s$ denotes the

POVM element for such system corresponding to the detector D_s clicking [37]. In this respect, $\hat{F}_s^\dagger \hat{F}_s$ takes the role of a generalised efficiency operator, such that when the system T is in a state $|\gamma\rangle_T$, the efficiency η_s of detector D_s is given by

$$\eta_s := \langle\gamma|\hat{F}_s^\dagger \hat{F}_s|\gamma\rangle_T. \tag{3}$$

Note that when $\hat{F}_s^\dagger \hat{F}_s = \eta_s \hat{\mathbb{1}}$, with $\eta_s \in [0,1]$, we obtain a model for detectors with constant efficiencies, which might be different for D_0 and D_1. While this description might not be the most general one, it well captures how the detectors functioning depends on additional modes and allows to investigate any scenario in which the information-carrying degree of freedom can be decoupled from the efficiency-affecting one.

We assume Bob can characterise his two detectors by performing an efficiency tomography measurement, and thus he learns the POVM elements $\{\hat{F}_s^\dagger \hat{F}_s\}_s$. We also assume $\hat{F}_0$ and $\hat{F}_1$ to be invertible, as no positive SKR can be achieved when this requirement is not satisfied [37].

(A6) We consider the asymptotic case where Alice sends to Bob an infinite number of signals and investigate coherent attacks.

Assumptions (A1)–(A2) imply that Alice knows precisely the states that are sent to the channel in each round of the protocol. On the receiver side, assumptions (A3)–(A4)–(A5) imply that Bob's POVMs are known and are defined over the tensor product space of systems B and T, being the former a qubit space. Importantly, we remark that our work is fully compatible with the decoy-state method for QKD [44–48], as the latter allows to estimate relevant probabilities related to single-photon signals.

3. Protocol description

In this section we introduce the fundamentals of the P&M three-state protocol which we base our analysis upon. We adopt the LT scheme, which considers basis mismatched events, and shall refer to it as the *actual protocol* in the following. Note that in the asymptotic regime, the phase-error rate for this scheme is the same as for the standard BB84 protocol [49].

Together with the actual protocol, we introduce a *virtual protocol* which is completely equivalent from Eve's viewpoint and allows for the phase-error rate estimation. Importantly, we fictitiously consider this protocol only for the purpose of the security proof and there is no need to actually implement it.

Actual Protocol

1. State preparation: Alice selects the Z (X) basis with probability p_{Z_A} (p_{X_A}). When the Z basis is selected, she prepares a single-photon pulse in the state $|\phi_{0_Z}\rangle_B$ or $|\phi_{1_Z}\rangle_B$ uniformly at random, whereas a single-photon pulse is prepared in the state $|\phi_{0_X}\rangle_B$ for the X basis selection. Then, she sends the single-photon pulse to Bob through a quantum channel. She repeats this step N times.
   Together with the B system, Bob receives from the channel an auxiliary T system which encodes information about the efficiency-affecting mode.
2. Measurement: For each pulse he receives, Bob selects the Z (X) basis with probability p_{Z_B} (p_{X_B}). Then, when the Z (X) basis is selected, he performs a measurement $\hat{M}^Z_{BT}$ ($\hat{M}^X_{BT}$) described by the POVM $\{\hat{M}^{0_Z}_{BT}, \hat{M}^{1_Z}_{BT}, \hat{M}^{\text{fail}_Z}_{BT}\}$ $\left(\{\hat{M}^{0_X}_{BT}, \hat{M}^{1_X}_{BT}, \hat{M}^{\text{fail}_X}_{BT}\}\right)$ over systems B and T. The POVM elements $\hat{M}^{s_\beta}_{BT}$ for $s \in \{0,1\}$ and $\beta \in \{X,Z\}$ are described by equation (1). The measurement outcomes corresponding to these operators are defined as detection events. On the other hand, $\hat{M}^{\text{fail}_\beta}_{BT}$ corresponds to an inconclusive event in the basis β. Note that due to DEM we have that $\hat{M}^{\text{fail}_X}_{BT} \neq \hat{M}^{\text{fail}_Z}_{BT}$.
3. Sifting: Once the previous steps are completed, Bob announces to Alice over an authenticated public channel in which rounds he obtained detection events, as well as the basis selection he made for each of these. This way, they can compute the sifted key, defined as the bit string generated from the instances in which Alice selected the Z basis and Bob obtained a detection event in the Z basis. Bob also shares with Alice a fraction of his results, allowing her to compute the probabilities associated to each possible detection event for each type of signal sent. Formally, we denote as $p_{s_\beta,i}$ the joint probability of Bob obtaining an outcome s_β, with $s \in \{0,1\}$ and $\beta \in \{X,Z\}$, and Alice sending the signal $i \in \{0_Z, 1_Z, 0_X\}$.
4. Parameter estimation: By using the estimated probabilities for measurements in the X basis $\{p_{s_X,i}\}_{s,i}$, Alice estimates an upper bound on the phase-error rate of the sifted key, while she estimates the bit-error rate in the Z basis through the values of $\{p_{s_Z,i}\}_{s,i}$ for $i \in \{0_Z, 1_Z\}$. These are the crucial parameters for privacy amplification and error correction, respectively.

5. Data-postprocessing: Through discussions over an authenticated public channel, Alice and Bob perform error correction, and then they conduct privacy amplification to generate a secret key.

The following virtual scheme is based on an equivalent entanglement-based (or source-replacement) approach. Crucially, Eve cannot distinguish this protocol from the actual one, as both the quantum and classical information available to Eve is the same for both protocols. Moreover, all the data that Alice and Bob use for the phase-error rate estimation (that is, all of Alice and Bob's detection data except for the sifted key) are also the same for both schemes. As a result, the phase-error rate estimated from the virtual protocol can be employed to determine the amount of privacy amplification needed to generate a secret key in the actual protocol [62, 63].

Virtual Protocol

1. Distribution of entanglement: Alice prepares bipartite systems, each of which is composed of a shield system A and a single-photon pulse B, in a joint entangled state in the form

$$|\varphi\rangle_{AB} = \sum_{c=1}^{6} \sqrt{p_c}\,|c\rangle_A \left|\phi^{(c)}\right\rangle_B . \tag{4}$$

   Each projection of the shield system onto one of the orthonormal basis states $\{|c\rangle_A\}_{c\in\{1,\ldots,6\}}$ corresponds to a different configuration of the state $\left|\phi^{(c)}\right\rangle_B$ sent to Bob and of the measurement basis choice for him. Specifically, Alice's measurement outcome being $c \in \{1,2\}$ corresponds to the rounds in which both her and Bob select the Z basis. For the sake of estimating the phase-error rate, in these rounds Bob is allowed to replace his standard Z basis measurement with a so-called virtual X basis measurement over systems B and T [62]. Details on the analytical form of this measurement are reported below. When Alice's outcome is $c \in \{3,4,5\}$, she is actually sending the states $|\phi_{0_Z}\rangle_B$, $|\phi_{1_Z}\rangle_B$ and $|\phi_{0_X}\rangle_B$, respectively, while Bob performs the same X basis measurement $\hat{M}^X_{BT}$ as in the actual protocol. Finally, Alice's outcome $c=6$ corresponds to her sending $|\phi_{0_X}\rangle_B$ and Bob measuring in the Z basis. Further details on this state preparation procedure can be found in appendix A.1 and table 2.
   After the preparation, Alice sends the system B to Bob through a quantum channel, while keeping the shield system in her lab. She repeats this step N times.
2. Delayed state preparation and measurement: After transmission, Alice performs the projective measurement described by $\{|c\rangle\langle c|_A\}_c$ over each of the N systems A she holds.
3. Announcement of detection events and bases for sifting, parameter estimation and postprocessing: These phases are tackled as in the actual protocol. One can follow the scheme provided in figure 7 to relate the quantities $\{p_{s_\beta,i}\}_{s,\beta,i}$ introduced in the actual protocol to the statics of the virtual protocol for various values of c.

Bob's virtual X basis measurement includes two filtering operations acting on systems B and T, followed by a projective measurement on system B. We further elaborate on filtering operations in section 3.1. In detail, we consider Bob first performing the filtering described by $\{\hat{Q}_Z = \sqrt{\hat{\mathbb{1}} - \hat{M}^{\text{fail}_Z}_{BT}}, \sqrt{\hat{M}^{\text{fail}_Z}_{BT}}\}$, followed by another (virtual) filtering operation $\{\hat{G}_{BT}, \sqrt{\hat{\mathbb{1}} - \hat{G}^\dagger_{BT}\hat{G}_{BT}}\}$ and finally by the projective measurement $\{|0_X\rangle\langle 0_X|_B \otimes \hat{\mathbb{1}}_T, |1_X\rangle\langle 1_X|_B \otimes \hat{\mathbb{1}}_T\}$. The analytical form of $\hat{G}_{BT}$ is introduced in equation (B20).

3.1. Filtering operations

Formally, a filtering operation is defined as a set of two Kraus operators $\left\{\hat{Q}_s, \hat{Q}_f\right\}$ (respectively, success and fail operators) acting on a given system S_1 in a state $|x\rangle_{S_1}$ such that, with a certain probability $p_s \leqslant 1$, the final state of the system is given by $\hat{Q}_s|x\rangle_{S_1}$ [64]. This is equivalent to considering an additional system S_2 and defining an unitary operation on the joint system $S_1 \otimes S_2$ in the form

$$U|x\rangle_{S_1}|0\rangle_{S_2} = \hat{Q}_s|x\rangle_{S_1} \otimes |s\rangle_{S_2} + \hat{Q}_f|x\rangle_{S_1} \otimes |f\rangle_{S_2}, \tag{5}$$

for any state $|x\rangle_{S_1}$. Here the (arbitrary) orthonormal states $|s\rangle_{S_2}$ and $|f\rangle_{S_2}$ for system S_2 denote success and failure of the filter, respectively. Crucially, this notion highlights how measuring the system S_2 after applying the filtering allows to immediately assert whether the filtering was successful. It follows from equation (5) that the probability of successful filtering can be found as

$$p_s := \langle x|\hat{Q}_s{}^\dagger \hat{Q}_s|x\rangle_{S_1} . \tag{6}$$

Importantly, through this paper we will address as 'filter' to a success operator $\hat{Q}_s$, therefore specifying only the evolution of a system in the case of successful filtering, since failure events are discarded. Note that for a filter to be valid it is sufficient that $\hat{Q}_s\hat{Q}_s^\dagger \leqslant \hat{\mathbb{1}}$ (equivalently, $\hat{Q}_s^\dagger\hat{Q}_s \leqslant \hat{\mathbb{1}}$), as this implies the existence of a valid corresponding failure operator and thus guarantees the non-violation of the unitarity of quantum mechanics.

Following the approach in [37], in this work we adopt the so-called Procrustean method of filtering [65]. This choice is motivated by the fact that, due to the DEM, Bob's detectors do not project onto perfectly orthogonal states of the joint system BT. Procrustean filtering allows, with a success probability smaller than unity, to orthogonalise the initial states and therefore offers a convenient way to apply Koashi's security proof [62]. More details on this matter can be found in appendix A.2.

4. Main result

In this section we summarise the main results of our analysis, providing a straightforward way to compute the SKR from experimental data. The proof of these results can be found in appendix B.

Let us consider the protocol introduced in section 3 and assume that the requirements in section 2 are met. Let $\boldsymbol{V}_i = (V_i^x, 0, V_i^z)^{\mathrm{T}}$ denote the Bloch vector of the state $|\phi_i\rangle_{\mathrm{B}}$, with $i \in \{0_Z, 1_Z, 0_X\}$. We define

$$p_3 = p_4 := \frac{p_{Z_A} p_{X_B}}{2}, \qquad p_5 := p_{X_A} p_{X_B}, \tag{7}$$

and

$$\tilde{\boldsymbol{q}}_s = \begin{pmatrix} \tilde{q}_{s_X,\mathbb{1}} \\ \tilde{q}_{s_X,X} \\ \tilde{q}_{s_X,Z} \end{pmatrix} := \begin{pmatrix} p_3 & p_3 V^x_{0_Z} & p_3 V^z_{0_Z} \\ p_4 & p_4 V^x_{1_Z} & p_4 V^z_{1_Z} \\ p_5 & p_5 V^x_{0_X} & p_5 V^z_{0_X} \end{pmatrix}^{-1} \begin{pmatrix} p_{s_X,0_Z} \\ p_{s_X,1_Z} \\ p_{s_X,0_X} \end{pmatrix}, \tag{8}$$

for $s \in \{0,1\}$.

Now, consider the unitary diagonalisation of the following Gram matrix

$$\hat{F}_0 \left(\hat{F}_1{}^\dagger \hat{F}_1\right)^{-1} \hat{F}_0^\dagger = \hat{U}\hat{D}\hat{U}^\dagger, \tag{9}$$

such that $\hat{D} = \mathrm{diag}\,(D_1, D_2, \ldots)$, with $D_i \geqslant 0\ \forall i$. Let us define

$$\hat{C} := \hat{C}_1 \hat{U}^\dagger \hat{F}_0, \tag{10}$$

where

$$\hat{C}_1 = \mathrm{diag}\,(\sqrt{\eta_1}, \sqrt{\eta_2}, \ldots), \qquad \eta_i := \min\left(\frac{1}{D_i}, 1\right). \tag{11}$$

Moreover, consider a set of four real, non-negative values $\boldsymbol{\Lambda} = \{\lambda_s^-, \lambda_s^+\}_{s\in\{0,1\}}$ such that

$$\lambda_s^- \hat{F}_s{}^\dagger \hat{F}_s \leqslant \hat{C}^\dagger \hat{C} \leqslant \lambda_s^+ \hat{F}_s{}^\dagger \hat{F}_s, \tag{12}$$

for $s \in \{0,1\}$.

Then, for the general case of coherent attacks, the asymptotic SKR per signal sent R is lower bounded as

$$R \geqslant p_Z^{\mathrm{sift}} \left[r_X^{\mathrm{virt},L} \left(1 - h_2\left(e_p^U\right)\right) - f h_2\left(e_b\right)\right], \tag{13}$$

where

$$p_Z^{\mathrm{sift}} := \sum_{s=0}^{1} \left(p_{s_Z,0_Z} + p_{s_Z,1_Z}\right) \tag{14}$$

is the probability of being in a sifted key round, the term $r_X^{\mathrm{virt},L}$ denotes a lower bound on the fraction of sifted key rounds in which Bob's virtual X basis measurement is successful (that is, the fraction of sifted key rounds for which Bob succeeds in making a guess for Alice's virtual X measurement outcome), $h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ denotes the binary entropy, e_p^U is an upper bound on the phase-error rate, f is the efficiency parameter associated to the error correction process and e_b is the bit-error rate. The latter quantity

can be directly inferred from the estimates of the detection probabilities in the sifted key rounds and is given by

$$e_b := \frac{p_{0_Z,1_Z} + p_{1_Z,0_Z}}{p_Z^{\text{sift}}}. \tag{15}$$

As for the bounds $r_X^{\text{virt},L}$ and e_p^U, let us first define

$$p_X^{\text{virt},L} := p_{Z_A} p_{Z_B} \left[\langle \phi_{0_Z} | \phi_{1_Z} \rangle \left(\frac{\lambda_0^+ + \lambda_0^-}{2} \tilde{q}_{0_X,X} + \frac{\lambda_1^+ + \lambda_1^-}{2} \tilde{q}_{1_X,X} \right) - \left(\frac{\lambda_0^+ - 3\lambda_0^-}{2} \tilde{q}_{0_X,\mathbb{1}} + \frac{\lambda_1^+ - 3\lambda_1^-}{2} \tilde{q}_{1_X,\mathbb{1}} \right) \right], \tag{16}$$

corresponding to a lower bound on the average of the conditional probabilities of the filters in Bob's virtual X measurement introduced in section 3 being successful, given Alice and Bob's outcomes in the previous rounds of the virtual protocol. Then, we have that

$$r_X^{\text{virt},L} = \frac{p_X^{\text{virt},L}}{p_Z^{\text{sift}}}, \tag{17}$$

while for the upper bound on the phase-error rate we have that

$$\begin{aligned} e_p^U = \frac{p_{X^{\text{virt}}}^{\text{err},U}}{p_X^{\text{virt},L}} := \frac{1}{p_X^{\text{virt},L}} \Bigg[& \frac{1 - \langle \phi_{0_Z} | \phi_{1_Z} \rangle}{2} \left(\frac{3\lambda_0^+ - \lambda_0^-}{2} \tilde{q}_{0_X,\mathbb{1}} - \frac{\lambda_0^+ + \lambda_0^-}{2} \tilde{q}_{0_X,X} \right) \\ & + \frac{1 + \langle \phi_{0_Z} | \phi_{1_Z} \rangle}{2} \left(\frac{3\lambda_1^+ - \lambda_1^-}{2} \tilde{q}_{1_X,\mathbb{1}} + \frac{\lambda_1^+ + \lambda_1^-}{2} \tilde{q}_{1_X,X} \right) \Bigg], \end{aligned} \tag{18}$$

where $p_{X^{\text{virt}}}^{\text{err,U}}$ denotes an upper bound on the average of the conditional probabilities of Bob making an error in his predictions in the virtual X measurement.

Although any choice of $\mathbf{\Lambda}$ satisfying equation (12) is a valid choice, one should pick the values that maximise the SKR. Nevertheless, as equations (16)–(18) depend on the experimental data through the estimates of $\{p_{s_\beta,i}\}_{s,\beta,i}$ (and, thus, $\tilde{\boldsymbol{q}}_s$), finding the optimal set $\mathbf{\Lambda}$ might be non-trivial. Nevertheless, we note that the term $p_X^{\text{virt},L}$ in equation (16) appears both at the numerator of equation (17) and at the denominator of equation (18), and thus we conjecture that maximising this quantity over the possible values of $\mathbf{\Lambda}$ corresponds to an optimisation of the SKR. This has a great impact since $p_X^{\text{virt},L}$ is a linear combination of the parameters in $\mathbf{\Lambda}$ and, crucially, the constraints on $\mathbf{\Lambda}$ given by equation (12) are semidefinite constraints on linear operators. Therefore, one can find suitable values of $\mathbf{\Lambda}$ by employing semidefinite programming, which allows for a fast and efficient optimisation. In detail, the semidefinite program (SDP) to solve is defined as

$$\begin{aligned} \text{maximise} \quad & p_X^{\text{virt},L}, \\ \text{subject to} \quad & \lambda_s^- \hat{F}_s{}^\dagger \hat{F}_s \leqslant \hat{C}^\dagger \hat{C}, \; s \in \{0,1\}, \\ & \hat{C}^\dagger \hat{C} \leqslant \lambda_s^+ \hat{F}_s{}^\dagger \hat{F}_s, \; s \in \{0,1\}, \\ & p_X^{\text{virt},L} \leqslant p_Z^{\text{sift}}, \\ & p_{X^{\text{virt}}}^{\text{err},U} \leqslant \tfrac{1}{2} p_X^{\text{virt,L}}. \end{aligned} \tag{19}$$

The second to last condition of the SDP above implies that $r_X^{\text{virt},L} \leqslant 1$, which is due to the fact that Bob performs a virtual X measurement for the sifted key rounds and therefore the probability of being in these rounds upper bounds the probability of Bob's virtual X measurement being successful. The last condition implies that the maximum phase-error rate allowed is $1/2$, corresponding to a uniformly random guess.

As an alternative to solving the SDP in equation (19), in appendix B we prove that valid lower and upper analytical bounds for $\hat{C}^\dagger \hat{C}$ in equation (12), although possibly suboptimal, are obtained for

$$\begin{aligned} \lambda_0^- &= \min\left(D_{\max}^{-1}, 1\right), \quad \lambda_0^+ = \min\left(D_{\min}^{-1}, 1\right), \\ \lambda_1^- &= \min\left(D_{\max}^{-1}, 1\right) D_{\min}, \quad \lambda_1^+ = \min\left(D_{\min}^{-1}, 1\right) D_{\max}, \end{aligned} \tag{20}$$

where $D_{\max}$ ($D_{\min}$) is the maximum (minimum) eigenvalue of the operator $\hat{D}$ introduced in equation (9).

Importantly, we remark that in the optimisation given by equation (19) we are not optimising the SKR directly, therefore the theory of SDP does not guarantee that the values of $\mathbf{\Lambda}$ found through this algorithm

are the optimal for equation (13). Nevertheless, they are suitable values whose performance can be directly compared with the ones in equation (20).

In the next section we show a direct application of our analysis, together with the computation of $\mathbf{\Lambda}$ through both equations (19) and (20).

5. Experimental characterisation and key rate simulation

To illustrate the applicability of our method, we compute numerically the SKR based on the experimental characterisation of two commercial SPDs. In detail, we consider the DEM induced by the detectors response to different polarisation states for the incoming photons. We employ two ID Qube NIR Free Running single-photon avalanche diodes (SPADs) produced by the company ID Quantique [66]. For both units, the nominal single-photon detection efficiency is set to $\eta_{th} = 25\%$ and the dead time to $\tau_d^{th} = 20\ \mu$s.

While this choice of detectors is motivated by the availability of equipment in our lab, we remark that the polarisation-induced DEM of SPADs is widely recognised as small compared with the one of superconducting nanowire SPDs [67], for which it would be of interest to conduct an analogous analysis.

5.1. Probing the polarisation-induced DEM

In this analysis we adopt the standard detector model depicted in figure 1. In detail, the single-photon detection efficiency $\eta \leqslant 1$ is modelled as the action of a beam splitter (BS) of equal transmittance, placed before a unitary efficiency detector (UED). As in our case we are investigating polarisation-dependent detection efficiency, the action of the BS depends on the polarisation state of the incoming light.

Consider a flux of photons arriving at the UED at an average rate R'_{in}, measured in photons per second (s^{-1}) or, equivalently, per arbitrary time unit. Let τ_d denote the actual detector dead time. Following the analysis carried out in [68], the average rate of total detected photons is given by

$$R_{\text{det}} = \frac{R'_{\text{in}}}{1 + R'_{\text{in}}\tau_d}. \tag{21}$$

Suppose now that the detector receives from the channel a train of single-photon states at a rate $R_{\text{in,sp}}$. At each round, the input state $\hat{\rho}$ in figure 1 is given by $\hat{\rho}_{\text{sp}} = |1\rangle\langle 1|$, with $|1\rangle$ being the single-photon Fock state. This means that after the BS the state becomes

$$\hat{\rho}'_{\text{sp}} = \eta\,|1\rangle\langle 1| + (1-\eta)\,|vac\rangle\langle vac|\,, \tag{22}$$

the latter term denoting the vacuum state. As a result, it can be considered that the UED receives photons at an incident rate $R'_{\text{in}} = \eta R_{\text{in,sp}} + R_{\text{dark}}$, since dark counts can be modelled as sporadic photons reaching the detector. Substitution in equation (21) yields a model to characterise the single-photon detection efficiency and the dead time of the detector by measuring the value of R_{det} for different incoming photon rates and then interpolating the experimental data.

Crucially, performing this characterisation would require a reliable single-photon source. In our case, we adopt a standard laser which is gain-switched at a repetition rate $\nu = 80$ MHz and is successively attenuated to the single photon level. Note that since $\nu \gg 1/\tau_d^{th}$, the detector sees the incoming light as a continuous wave. Nevertheless, by pulsing the laser we mitigate beating effects due to reflections in the optical line, which might induce fluctuations of the average intensity that ultimately alter the results. In fact, a laser operating in continuous-wave mode can suffer from 'cavity effects' due to imperfect fiber connections that can cause multiple weak reflections which interfere with the original signal from the source, thus leading to fluctuations in the optical power arriving at the detector. This effect is greatly minimized when the laser is pulsed, since due to gain-switching the pulses have an approximately uniformly random phase relation, and thus the average power at the detectors is more stable.

Adopting a pulsed laser source, the signal arriving at the detector at each round consists of a weak coherent pulse of intensity μ. Going through the BS in figure 1, which models the non-ideal efficiency, causes an attenuation of the intensity $\mu \to \eta\mu$, which means that after the BS the state of the pulse takes the form

$$\hat{\rho}'_{\text{ch}} = \left|\sqrt{\eta\mu}e^{i\phi}\right\rangle\!\left\langle\sqrt{\eta\mu}e^{i\phi}\right| = e^{-\eta\mu}\sum_{n,m=0}^{\infty}\frac{\left(\sqrt{\eta\mu}\right)^{n+m}e^{i(n-m)\phi}}{\sqrt{n!m!}}\,|n\rangle\langle m|\,, \tag{23}$$

where the last expression corresponds to the state expansion in the Fock basis. This implies that the probability of not being in a vacuum state is given by

$$\sum_{k=1}^{\infty}\langle k|\hat{\rho}'_{\text{ch}}|k\rangle = 1 - e^{-\eta\mu} \overset{\eta\mu\ll 1}{\approx} \eta\mu, \tag{24}$$

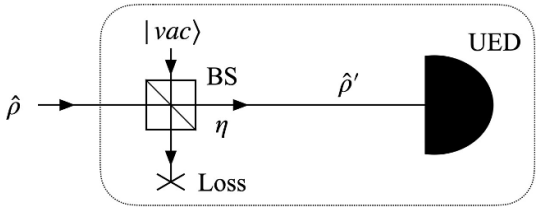


Figure 1. Modelling of a realistic SPD (dotted box). The input state $\hat{\rho}$ goes first through a beam splitter (BS) of transmittance η, which models the limited detector efficiency as the coupling of the input mode and the vacuum state ($|vac\rangle$) with a lost line. Afterwards, the light is directed towards a unitary efficiency detector (UED) which has realistic dead time and dark count rate.

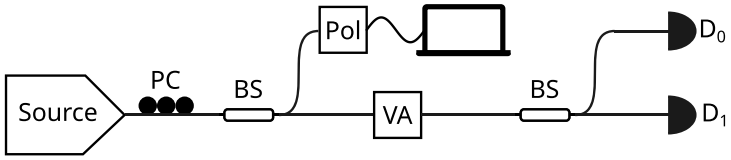


Figure 2. Experimental setup for the characterisation of the polarisation-dependent DEM of two detectors D_0 and D_1. Here PC, polarisation controller; Pol, polarimeter; BS, balanced beam splitter; VA, variable attenuator.

where the final approximation holds in our case since, for all the data acquisition rounds we perform, the value of μ satisfies $\mu \leqslant 0.1$. Therefore, we have that the average rate of incoming photons to the UED is given by

$$R'_{\text{in}} \approx \eta\mu\nu + R_{\text{dark}} = \eta R_{\text{in,ch}} + R_{\text{dark}}, \tag{25}$$

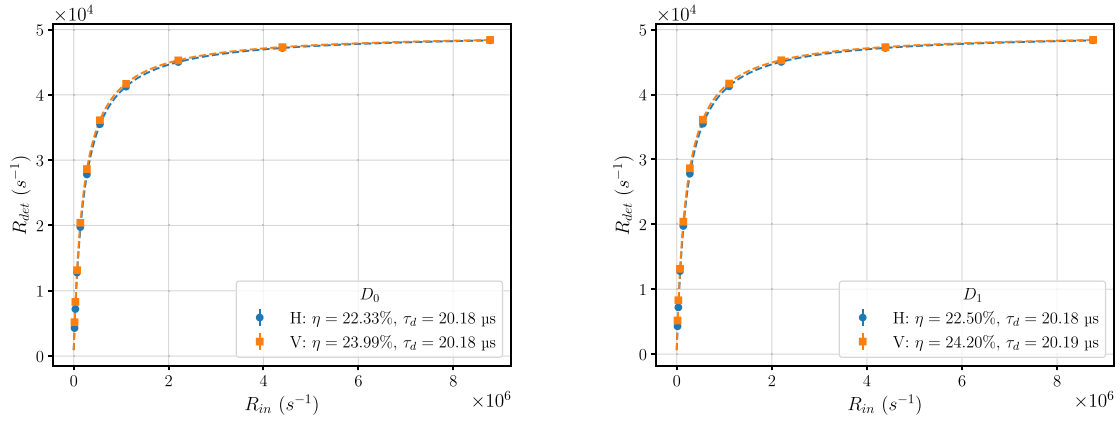
where we have defined the average rate of photons sent to the detector in the case of coherent light $R_{\text{in,ch}} := \mu\nu$. For ease of notation, in the following we neglect the subscript ch.

To measure the average count rate of the detectors while changing the rate and the polarisation state of the incoming photons we adopt the fiber-based scheme described in figure 2. Here, we study four polarisations states, namely horizontal ($|H\rangle$), vertical ($|V\rangle$), diagonal ($|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$) and circular-left ($|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$), as they suffice in providing a full tomography of the operators $\{\hat{F}_s^{\dagger}\hat{F}_s\}_{s\in\{0,1\}}$. For each polarisation, we measure the average amount of detected photons per second over a 10 s time window. The measured dark counts rates of the two SPDs over such time window are 930 s^{-1} and 630 s^{-1}, respectively. We note that since we do not employ polarisation-maintaining fiber, the polarisation state at the entrance of the SPDs might be, in all generality, different from the one measured by the polarimeter in figure 2, up to a unitary transformation. Hence, the basis adopted for the characterisation of the SPDs is the one of the polarisation states at the polarimeter.

For illustration purposes, we depict the results of this analysis for the case of horizontal and vertical polarisations in figure 3. The full results are reported in table 1. We remark that these values only serve the purpose of explaining the application of our analysis and, as such, performing a more extensive parameter estimation with high precision and small uncertainty goes beyond the scope of this paper. On this note, table 1 seems to suggest that the dead time of detector D_1 depends on the polarisation of the incoming light. However, all dead time estimates can be considered equivalent within the statistical error coming from the parameter estimation, which means that there is no experimental evidence of the dead time of the detectors being polarisation-dependent, given the precision of the measurements.

Importantly, we observe a systematic decrease of both detectors efficiency for the polarisation state $|H\rangle$. This could be due to a joint DEM of the two detectors, or to polarisation-dependent losses in the elements of the optical line that we employ in our characterisation setup (see figure 2). In detail, we have experimentally measured intensity fluctuations at the detectors entrance up to 5% when changing the polarisation, which are compatible with the nominal polarisation-dependent loss in the BSs we adopt, which is up to 0.2 dB according to the manufacturer. Nevertheless, BSs are typically part of the measurement scheme and, in all generality, for the sake of proving the implementation security it is meaningful to consider the worst case scenario, that is, the one in which the discrepancy in efficiency we observe is due to polarisation-dependent DEM of the SPDs.

It follows from Assumption (A5) that the efficiency of the detector D_s for $s \in \{0,1\}$ when the incoming photons are in a polarisation state $|\sigma\rangle \in \{|H\rangle, |V\rangle, |D\rangle, |L\rangle\}$ can be found through equation (3) to be



(a) Detector D_0. (b) Detector D_1.

Figure 3. Experimental data for the characterisation of the efficiency of detectors D_0 (figure 2(a)) and D_1 (figure 2(b)), considering horizontal and vertical polarisation of the incoming light. We interpolate the experimental data (full markers) with the model given by equations (21)–(25) (dashed lines) through the non-linear least squares method. The efficiency η and the dead time τ_d are then estimated as the optimal parameters of the interpolation. We note that error bars associated to the experimental points in these plots, which correspond to the standard deviation of the measurements over the time window, are not quite visible, as they are approximately 1% of the detected values.

Table 1. Results of the characterisation of the detection efficiency of two SPADs when changing the polarisation of the incoming light. The values in this table are obtained as the optimal parameters of the interpolation of the function in equations (21) and (25) over the experimental data. The relative error (i.e. the statistical error normalised to the measured value) in the estimates of η is about 1% for all data acquisitions, while the one of τ_d is of the order of 0.05%.

	H		V		D		L	
	η	τ_d (μs)	η	τ_d (μs)	η	τ_d (μs)	η	τ_d (μs)
D_0	22.33%	20.18	23.99%	20.18	23.78%	20.18	23.69%	20.18
D_1	22.50%	20.18	24.20%	20.19	24.01%	20.19	23.86%	20.18

$\eta_s^\sigma := \langle\sigma|\hat{F}_s{}^\dagger\hat{F}_s|\sigma\rangle$. Therefore, the analytical form of $\{\hat{F}_s{}^\dagger\hat{F}_s\}_{s\in\{0,1\}}$ can be computed from the experimental data as

$$\hat{F}_s{}^\dagger\hat{F}_s = \begin{pmatrix} \alpha_s & \beta_s \\ \beta_s^* & \gamma_s \end{pmatrix}, \qquad \text{with} \qquad \begin{cases} \alpha_s = \eta_s^H \\ \gamma_s = \eta_s^V \\ \mathrm{Re}\,(\beta_s) = \eta_s^D - \frac{1}{2}\left(\eta_s^H + \eta_s^V\right) \\ \mathrm{Im}\,(\beta_s) = \frac{1}{2}\left(\eta_s^H + \eta_s^V\right) - \eta_s^L. \end{cases} \tag{26}$$

Combining equation (26) with the data provided in table 1 gives the efficiency matrices of the two detectors:

$$\hat{F}_0{}^\dagger\hat{F}_0 = \begin{pmatrix} 0.2233 & 0.0062 - 0.0052j \\ 0.0062 + 0.0052j & 0.2399 \end{pmatrix}, \tag{27}$$

$$\hat{F}_1{}^\dagger\hat{F}_1 = \begin{pmatrix} 0.2250 & 0.0066 - 0.0051j \\ 0.0066 + 0.0051j & 0.2420 \end{pmatrix}, \tag{28}$$

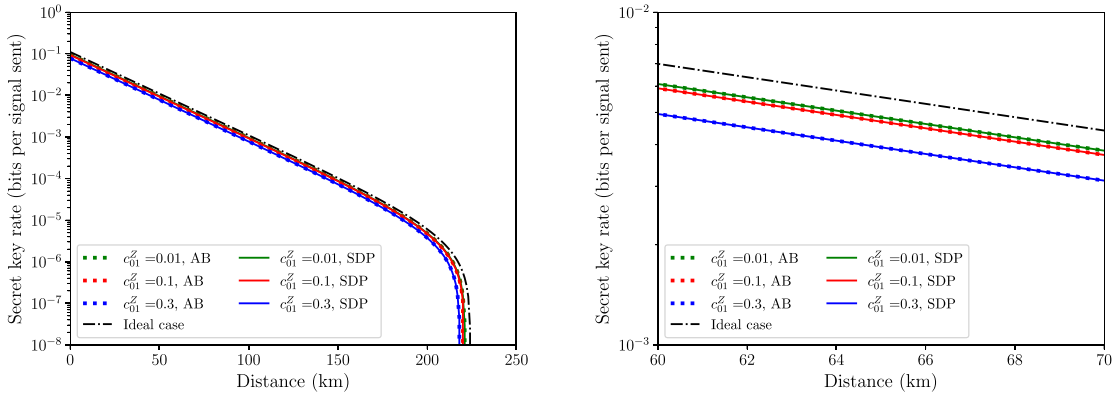
while the operators $\{\hat{F}_s\}_s$ for $s \in \{0,1\}$ can be found from the diagonalisation of the hermitian matrices in equations (27) and (28) as

$$\hat{F}_s{}^\dagger\hat{F}_s = \hat{U}_s^\dagger\hat{D}_s\hat{U}_s, \qquad \hat{F}_s = \hat{D}_s^{1/2}\hat{U}_s. \tag{29}$$

The maximum and minimum efficiency of the detectors can be found as the maximum and minimum eigenvalues of the operators in equations (27) and (28). By computing them, one finds that the efficiency ranges for D_0 and D_1 are $[22.00\%, 24.32\%]$ and $[22.16\%, 24.54\%]$, respectively.

5.2. SKR simulation

To compute the SKR, we consider the case of a time-bin-encoding three-state protocol. To simulate the detection statistics, we focus on the case in which Eve manipulates the polarisation of the incoming light



(a) Full view. (b) Zoomed view.

Figure 4. Lower bound on the asymptotic SKR for the three-state protocol with SPFs and DEM corresponding to the detector matrices reported in equations (27) and (28). The results are obtained through the analysis in section 4, considering an efficiency of the error correction code $f = 1.16$. We compare the performance of our approach adopting the values of $\mathbf{\Lambda}$ provided by the analytical bounds (AB) in equation (20) (dashed lines) with the values given by the SDP in equation (19) (solid lines). The black dash-dotted line corresponds to the results for identical detectors working at the nominal efficiency (i.e. $\hat{F}_0{}^\dagger \hat{F}_0 = \hat{F}_1{}^\dagger \hat{F}_1 = 25\%$) and no SPFs. From the full picture (figure (a)) it looks clear that the estimated DEM does not affect the performance greatly. By looking in more detail (figure (b)), we can observe, as expected, that higher SPFs correspond to lower SKR. Moreover, for the case we are considering, the results adopting the terms $\mathbf{\Lambda}$ obtained thought analytical bounds and SDP coincide.

without affecting the signal state prepared by Alice. Formally, this corresponds to the case in which at every round

$$|\phi_i\rangle_B |\sigma_0\rangle_T \xrightarrow{\text{Eve}} |\phi_i\rangle_B |\sigma_E\rangle_T, \tag{30}$$

where $i \in \{0_Z, 1_Z, 0_X\}$, $|\sigma_0\rangle_T$ denotes the (arbitrary) polarisation of the pulses sent by Alice and $|\sigma_E\rangle_T$ is the polarisation state set by Eve. For concreteness, we choose the scenario in which Eve selects $|\sigma_E\rangle_T$ as the eigenstate corresponding to the minimum eigenvalue of $\hat{F}_1{}^\dagger \hat{F}_1$, effectively forcing D_1 to operate at the minimum possible detection efficiency. In this case, the probability of each detector clicking when receiving a photon is given by

$$\eta_0^{\sigma_E} := \langle \sigma_E | \hat{F}_0{}^\dagger \hat{F}_0 | \sigma_E \rangle = 22.01\%, \qquad \eta_1^{\sigma_E} := \langle \sigma_E | \hat{F}_1{}^\dagger \hat{F}_1 | \sigma_E \rangle = 22.16\%. \tag{31}$$

To account for SPFs, we consider three possible values of the overlap of the flawed Z states given by

$$c_{01}^Z := \langle \phi_{0_Z} | \phi_{1_Z} \rangle_B \in \{0.01, 0.1, 0.3\}, \tag{32}$$

and study the case in which Alice sends her three states with equal *a priori* probability $p_i = 1/3$, while Bob measures the incoming signals in the Z basis with probability $p_{Z_B} = 2/3$. The joint probability of Alice sending the state i and Bob detecting s_β, with $s \in \{0,1\}$ and $\beta \in \{X, Z\}$, is then computed as

$$p_{s_\beta, i} = \frac{p_{\beta_B}}{3} \left[\eta_{\text{ch}} |\langle \phi_i | s_\beta \rangle|^2 \eta_s^{\sigma_E} \left(1 - \frac{p_{\text{dark}}}{2}\right) + p_{\text{dark}} \left(1 - \eta_{\text{ch}} |\langle \phi_i | s_\beta \rangle|^2 \eta_s^{\sigma_E}\right) \left(1 - \frac{p_{\text{dark}}}{2}\right) \right], \tag{33}$$

where $\eta_{\text{ch}} = 10^{-\alpha L/10}$ is the transmittance of a lossy channel of length L with attenuation coefficient $\alpha = 0.2$ dB/km for standard single-mode optical fiber. The value of p_{dark} has been set to 10^{-6}, corresponding to an upper bound on the dark count probability for these detectors in a QKD setup running at 1 GHz. Here we consider the case in which double clicks are randomly assigned to single clicks with equal probability [69].

With this choice of parameters we can compute the entries of the terms $\tilde{\boldsymbol{q}}_s$ in equation (8). To proceed to the calculation of the SKR given by equation (13), the only missing ingredient are the values of $\mathbf{\Lambda}$. For these, we both solve the SDP in equation (19) and obtain the analytical bounds provided by equation (20). The results are displayed in figure 4. Critically, we observe that the mismatches in the detectors efficiencies due to polarisation do not dramatically affect the performance of the protocol. This point is further investigated in the next section. Similarly, the role of SPFs is also mitigated, thanks to the LT approach. For the specific case under investigation, we also find that the results of the analytical bounds and SDP coincide, although in all generality this might not always be the case.

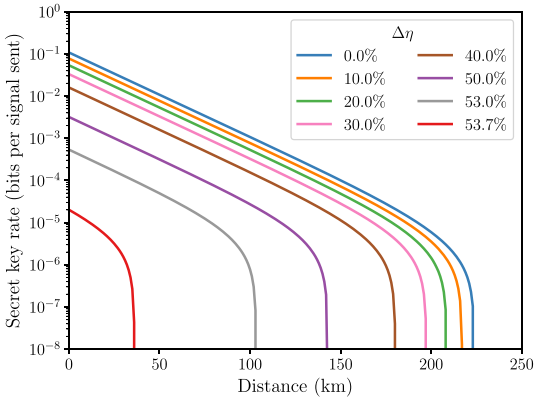


Figure 5. Lower bound on the asymptotic SKR for the three-state protocol with SPFs corresponding to $c_{01}^{Z} = 0.1$ and detector matrices reported in equation (34). The results are obtained through the analysis in section 4, solving the SDP in equation (19) and considering an efficiency of the error correction code $f = 1.16$. Results suggest that our analysis is capable of providing a secret key with a DEM greater than 50%, under the considered intensity of the SPFs.

Robustness against large DEM

All previous results in this section are based on the characterisation of realistic devices. Nevertheless, it is of interest to investigate as well how the performance of our proof is affected by larger DEM. To do so, we consider now the exemplificative case of a perfect detector D_0' working at the nominal efficiency of 25% for all polarisation states, and a faulty detector D_1' whose efficiency in a particular (arbitral) polarisation state is changed. The polarisation-dependent efficiency operators in this case take the form:

$$\hat{F}_0'^{\dagger}\hat{F}_0' = \begin{pmatrix} 0.25 & 0 \\ 0 & 0.25 \end{pmatrix}, \qquad \hat{F}_1'^{\dagger}\hat{F}_1' = \begin{pmatrix} 0.25 & 0 \\ 0 & 0.25\,(1-\Delta\eta) \end{pmatrix}, \tag{34}$$

where $\Delta\eta$ denotes the relative DEM. We compute the SKR adopting our proof as illustrated in the previous section for an intermediate case of SPFs, that is, $c_{01}^{Z} = 0.1$.

Results are displayed in figure 5. We note that our analysis is robust against DEM of large magnitude, even in presence of significant SPFs. For the case at hand, the maximum tolerable relative DEM is about 53.7%, corresponding to a minimum efficiency for the detector D_1' of 11.58%.

6. Discussion

Results in section 4 show directly how both SPFs and DEM affect the SKR. Importantly, we find that in case of identical detectors it holds $\lambda_s^- = \lambda_s^+ = 1$ for $s \in \{0,1\}$, and thus we retrieve the results of the original LT work [49]. In this latter case, experimental data from the actual protocol where Bob measures in the X basis can be used to estimate the phase-error rate directly, due to the fact that the basis-independent detection efficiency condition holds.

We also note that in equation (9) the choice of which label ('0' or '1') is assigned to the physical devices is completely arbitrary, hence one should choose the labelling that maximises equation (13).

Crucially, while the non-orthogonality of the Z states directly affects the SKR, the deviation of $|\phi_{0_X}\rangle$ from $|0_X\rangle$ can be arbitrarily large, given that the state $|\phi_{0_X}\rangle$ is perfectly characterised. This is due to the fact that for the LT method the role of this state is only to help in the definition of the terms $\tilde{\boldsymbol{q}}_s$ in equation (8). In this respect, to achieve positive SKR Alice only needs to be able to prepare three pure states, select the most orthogonal ones as her key (Z) states and adopt the last one as trial state to compute the action of the channel on her signals.

It is important to remark the physical intuition behind the computation of the bounds in equations (17) and (18). The potential of the LT approach lays in the fact that events in which Alice selects the Z basis and Bob measures the incoming signals in the X basis, which are typically discarded, can be actually used to characterise the channel action on the travelling systems and, therefore, help to estimate the phase-error rate. In the presence of DEM, this cannot be done in a straightforward way, as different detection probabilities in the two bases make impossible to directly relate the statistics of Bob's Z and X basis measurements. The role of the Procrustean virtual filter is precisely to remove this imbalance of the detectors, such that a scenario in which the detectors are equal can be restored in the virtual scheme. From here, operational inequalities such as the one in equation (12) can be employed to relate the statistics of Bob's virtual X outcomes to his actual X

measurements, which he experimentally performs. This concept is illustrated in figure 9 and further discussed in appendix A.2.

In section 5.1 we illustrate the experimental procedure we carried out to estimate the detectors efficiencies for different polarisation states of light. In doing so, we also obtain estimates of the dead time of the detectors, finding the results that we report in table 1. We remark that the dead time does not play a direct role in our security proof, nor in the simulations of the SKR in figures 4 and 5. In fact, the way in which the dead time of the detectors impacts security is by limiting the rate at which Bob can detect events that contribute to the generation of the secret key. More in detail, in the time window of duration equal to the dead time which immediately follows a click, the detector is restoring its operational regime and, consequently, will not be able to detect any signal. This means that during this time window the efficiency of such detector is zero for any state of system T. As all events during this time interval can only trigger a detection in one of the two detectors, these cannot be considered secure [18]. Crucially, we underline how Bob receiving its signal when both detectors are active is an implicit requirement of Assumption (A5) being satisfied. This follows from the fact that the the efficiency of the detector D_s being zero for any state formally translates to $\hat{F}_s^\dagger \hat{F}_s \equiv 0$ (that is not invertible, as required in Assumption (A5)). In practice, to prevent that events recorded in this insecure time window are used to generate the raw key, it is recommended that the receiver is equipped with a mechanism (such as a shutter or a variable attenuator) that blocks pulses from reaching the detectors during the dead time, or continuously monitors if both detectors are active. Alternatively, under the assumption that Eve cannot increase the dead time of the detectors by injecting external light, one could simply analyse all events in the post-processing and discard the events whose detection time was less than one dead time away from the previous one.

7. Conclusions

In this paper, we have provided a security proof for the LT QKD protocol, incorporating imperfections in both the source and measurement devices. Specifically, we have considered a setup subject to both SPFs and DEM, for which the efficiency of the detectors varies according to several degrees of freedom of the received pulses, such as arrival time, frequency, polarisation, and spatial modes. Under assumptions on realistic SPFs and a experimentally-characterised polarisation-dependent DEM for commercial single-photon detectors, our security proof shows that small differences in the detectors efficiency do not affect much the key generation rate. In this respect, our work proves that LT QKD can be applied to setups with slightly unbalanced detection efficiency with minimal penalty.

We conclude this paper with some open questions. We first remark for future reference that a more comprehensive analysis might benefit of relaxation of some assumptions we made in section 2, particularly the restriction of the information-carrying system to a qubit space for both Alice (Assumption (A1)) and Bob (Assumption (A4)). Moreover, as in this work we have only considered SPFs, it is relevant to extend our security proof including also other major source imperfections, such as correlations among emitted pulses and side-channels [50–54]. Finally, our work provides a security proof in the asymptotic regime, where the number of emitted pulses is assumed to be infinite. From here, it will be of interest to conduct a security analysis for finite lengths. In this latter case, it should be noted that, as mentioned in the discussion leading to equation (B16), it is necessary to consider probability trials across the entire train of emitted pulses. This supports the use of Kato's inequality [70], which provides better convergence for finite lengths with respect to Azuma's inequality [71].

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors.

Acknowledgments

The authors thank G Currás-Lorenzo, M Pereira, Á Navarrete, X Sixto, D Rusca and V Makarov for insightful discussions. The work of A Marcomini is fully funded by the Marie Sklodowska-Curie Grant No. 101072637 (Project Quantum-Safe-Internet). Support from the Galician Regional Government (consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through the Grant No. PID2020-118178RB-C21, MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the 'Planes Complementarios de I+D+I con las Comunidades Autónomas' in Quantum Communication, and the European Union's Horizon Europe Framework Programme under the project 'Quantum Security Networks Partnership' (QSNP, Grant Agreement No.

101114043) is greatly acknowledged. A Mizutani is partially supported by JSPS KAKENHI Grant No. JP24K16977. K Tamaki acknowledges support from JSPS KAKENHI Grant No. 23H01096.

Appendix A. Setup model

In this appendix we present a brief description of the model we use to describe the transmitter and receiver components of the QKD system considered, relating them to the assumptions reported in section 2. The notation we introduce here is later used in appendix B for the proof of our results.

A.1. Transmitter

In a three-state QKD scheme, let $|\phi_{0_Z}\rangle$, $|\phi_{1_Z}\rangle$ and $|\phi_{0_X}\rangle$ denote the flawed quantum states prepared by Alice (which can be in principle different from the perfect $|0_Z\rangle$, $|1_Z\rangle$ and $|0_X\rangle$ states). These states are illustrated in figure 6. For later convenience, we make a choice of the axes of the Bloch sphere in such a way that all states share the same Y coordinate and $|\phi_{0_Z}\rangle$ and $|\phi_{1_Z}\rangle$ are symmetric with respect to the X axis. Note that this is always possible, given that the Bloch vectors of the flawed states are not all parallel (visually, this means that these states form a non-degenerate triangle on a plane cutting the Bloch sphere). Here we focus on the particular case of states laying on the XZ plane of the sphere, since any set of states sharing the same Y coordinate can be uniformly lifted to this plane through a filter $q|0_Y\rangle\langle 0_Y| + (1-q)|1_Y\rangle\langle 1_Y|$ with $0 \leqslant q < 1$. This ensures that $\langle\phi_{0_Z}|\phi_{1_Z}\rangle \in \mathbb{R}$.

Therefore, the Z states prepared by Alice for system B can be written as

$$|\phi_{a_Z}\rangle_B = \cos\left(\frac{\theta - a\pi}{2}\right)|0_Z\rangle_B + (-1)^a \sin\left(\frac{\theta - a\pi}{2}\right)|1_Z\rangle_B, \tag{A1}$$

for $a = 0, 1$ and an angle $\theta \in (-\pi, \pi]$ (see figure 6), which typically satisfies $|\theta| \ll 1$ in practical implementations.

Equivalently, we can consider Alice preparing the joint states

$$|\Psi_Z\rangle_{A'B} = \frac{1}{\sqrt{2}}\left(|0_Z\rangle_{A'}|\phi_{0_Z}\rangle_B + |1_Z\rangle_{A'}|\phi_{1_Z}\rangle_B\right), \tag{A2}$$

$$|\Psi_X\rangle_{A'B} = |0_X\rangle_{A'}|\phi_{0_X}\rangle_B, \tag{A3}$$

for a two-qubit system $A'B$. She then keeps the system A' in her lab, while sending the system B to Bob. When preparing $|\Psi_Z\rangle_{A'B}$, by measuring A' in the Z basis she eventually selects the state of system B.

Now, let the virtual X states of system B be defined as the balanced superposition of the actual Z states, namely

$$\left|\phi^{\text{virt}}_{0_X}\right\rangle_B := \frac{|\phi_{0_Z}\rangle_B + |\phi_{1_Z}\rangle_B}{\||\phi_{0_Z}\rangle_B + |\phi_{1_Z}\rangle_B\|} \equiv |0_X\rangle_B,$$

$$\left|\phi^{\text{virt}}_{1_X}\right\rangle_B := \frac{|\phi_{0_Z}\rangle_B - |\phi_{1_Z}\rangle_B}{\||\phi_{0_Z}\rangle_B - |\phi_{1_Z}\rangle_B\|} \equiv |1_X\rangle_B. \tag{A4}$$

We notice that these virtual X states coincide with the true $\hat{X}$ eigenstates, due to the fact that the flawed Z states are symmetric with respect to the X axis of the Bloch sphere. Since $|a_Z\rangle_{A'} = \left(|0_X\rangle_{A'} + (-1)^a|1_X\rangle_{A'}\right)/\sqrt{2}$ for $a \in \{0, 1\}$, the state $|\Psi_Z\rangle_{A'B}$ in equation (A2) can be rewritten as

$$|\Psi_Z\rangle_{A'B} = \sqrt{p_{0^{\text{virt}}_X}}|0_X\rangle_{A'}\left|\phi^{\text{virt}}_{0_X}\right\rangle_B + \sqrt{p_{1^{\text{virt}}_X}}|1_X\rangle_{A'}\left|\phi^{\text{virt}}_{1_X}\right\rangle_B, \tag{A5}$$

where $p_{0^{\text{virt}}_X}$ ($p_{1^{\text{virt}}_X}$) denotes the probability of Alice sending Bob the virtual state $\left|\phi^{\text{virt}}_{0_X}\right\rangle_B$ ($\left|\phi^{\text{virt}}_{1_X}\right\rangle_B$) in the virtual scenario. These probabilities are given by

$$p_{0^{\text{virt}}_X} = \frac{\||\phi_{0_Z}\rangle_B + |\phi_{1_Z}\rangle_B\|^2}{4} = \frac{1 + \langle\phi_{0_Z}|\phi_{1_Z}\rangle_B}{2},$$

$$p_{1^{\text{virt}}_X} = 1 - p_{0^{\text{virt}}_X}. \tag{A6}$$

Remarkably, equation (A5) highlights how measuring the virtual X states Bob could predict the outcome of an X measurement on Alice's system A', when she prepares $|\Psi_Z\rangle_{A'B}$. This is the core aspect of Koashi's security proof based on complementarity [62]. Moreover, although in practical applications Alice sends Bob the states $|\phi_{0_Z}\rangle_B$ and $|\phi_{1_Z}\rangle_B$ with equal *a priori* probability in the key rounds, the probability of sending the virtual X states are generally different (as clearly visible in figure 6, where the state $\left|\phi^{\text{virt}}_{0_X}\right\rangle$ is favored).

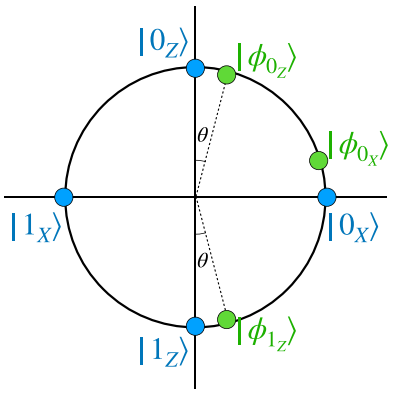


Figure 6. Illustration of the flawed quantum states $|\phi_i\rangle_{i\in\{0_Z,1_Z,0_X\}}$ for the B system prepared by Alice (in green). Due to imperfections in the state preparation process, they differ from the eigenstates of the $\hat{X}$ and $\hat{Z}$ Pauli matrices (in blue). The choice of the X and Z axes of the Bloch sphere is done in such a way that the states $|\phi_{0_Z}\rangle$ and $|\phi_{1_Z}\rangle$ are symmetric with respect to the X axis, i.e. they are rotated by the same angle θ from their ideal reference states.

As further discussed in appendix B, it is meaningful to study the evolution through the channel of all these states in the protocol, with a specific focus on the detection statistics in the X basis for the actual states and in the Z basis for the virtual states. For this, we define the virtual, equivalent scheme introduced in section 3. In this virtual scheme, an auxiliary shield system A is adopted to describe a total of six different configurations, each corresponding to a specific state sent by Alice and a measurement choice for Bob. This description allows us to use the same notation for the analysis of the actual states sent and the one of the virtual X states in equation (A4), which are not actually sent. In doing so, we have that the resulting state over the joint system AB is in the form introduced in equation (4), and measuring in the orthonormal basis $\{|c\rangle_A\}_{c\in\{1,\dots,6\}}$ of the shield system allows to select both a state $|\phi^{(c)}\rangle_B$ and a measurement basis for Bob. A summary of the virtual scheme is illustrated in figure 7, while the states $|\phi^{(c)}\rangle_B$, their corresponding probability and measurement basis are reported in table 2.

Following the model introduced in [37], we consider an additional system T which allows to characterise the nature of the efficiency mismatch. Intuitively, one can for example think of states $\{\dots,|-1\rangle_T,|0\rangle_T,|1\rangle_T,\dots\}$ representing delays in the time of arrival of the single-photon to Bob's detector, or $|\sigma\rangle_T$ denoting a polarisation state for the incoming light as studied in section 5, although this analysis applies to arbitrary mismatch-inducing modes. We shall introduce this system T in a trivial configuration $|0\rangle_T$, allowing Eve to fully act on it in the channel. As a result, at each round of the protocol the joint state of the three systems A, B and T at the output of the transmitter is

$$|\varphi\rangle_{ABT} = |\varphi\rangle_{AB} \otimes |0\rangle_T, \tag{A7}$$

with $|\varphi\rangle_{AB}$ given by equation (4).

A.2. Receiver

The operators $\hat{F}_s{}^\dagger \hat{F}_s$ acting on system T that appear in equation (1) represent the generalised efficiency of the two detectors [37]. Precisely, the quantity $\langle\gamma|\hat{F}_s{}^\dagger \hat{F}_s|\gamma\rangle_T$ represents the probability of the detector D_s clicking when the system T is in a state $|\gamma\rangle$. Note that Assumption (A3) in section 2 implies that the operators $\hat{F}_s{}^\dagger \hat{F}_s$ are the same in the Z and X basis, as the same physical device used to detect s_X is also employed to measure s_Z (thus having the same detection efficiency).

The measurements operators $\hat{M}_{BT}^{s_\beta}$ introduced in equation (1) can be equivalently modelled as the result of a filter

$$\hat{Q}_\beta = |0_\beta\rangle\langle 0_\beta|_B \otimes \left(\hat{F}_0\right)_T + |1_\beta\rangle\langle 1_\beta| \otimes \left(\hat{F}_1\right)_T, \tag{A8}$$

followed by a projection $|s_\beta\rangle\langle s_\beta|_B \otimes \hat{\mathbb{1}}_T$ on the system B. In fact, we have that

$$\hat{M}_{BT}^{s_\beta} = \hat{Q}_\beta^\dagger \left(|s_\beta\rangle\langle s_\beta|_B \otimes \hat{\mathbb{1}}_T\right) \hat{Q}_\beta. \tag{A9}$$

This is relevant because the filtering discriminates the 'successful' and 'failure' bit measurement outcome, while the following projective measurement simply assigns the bit value to successful events. This is due to

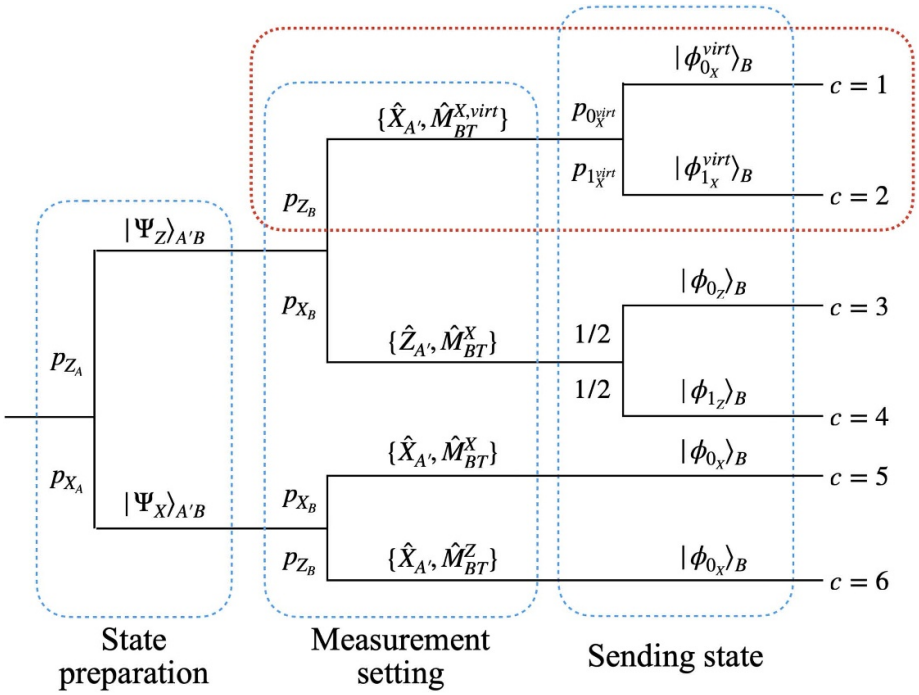


Figure 7. This diagram illustrates the six scenarios corresponding to the states $\{|c\rangle_A\}_{c\in\{1,\dots,6\}}$ in the virtual protocol introduced in section 3 and explains the quantities in the summary provided in table 2. Proceeding from left to right, Alice prepares the entangled states $|\Psi_Z\rangle_{A'B}$ and $|\Psi_X\rangle_{A'B}$ given by equations (A2) and (A3) with probability p_{Z_A} and p_{X_A}, respectively. Then, by performing a projective measurement $\hat{Z}_{A'}$ ($\hat{X}_{A'}$) in the Z (X) basis, she post-selects the sending state of the B system she is sending to Bob. For later use, here we already distinguish the possible measurement basis choices of Bob, including their probabilities in the definitions of the scenarios described by $c \in \{1,\dots,6\}$. From Assumption (A5) in section 2, Bob's measurements act on a joint system BT, being system T the one describing the efficiency-affecting mode. The red box refers to the case of Bob performing a virtual X basis measurement to predict the outcomes Alice would obtain by performing a measurement $\hat{X}_{A'}$ in the sifted key rounds ($c \in \{1,2\}$). The phase-error rate is defined in terms of these outcomes. As the virtual measurement involves the sifted key rounds, the probability of performing the virtual measurement is the same of Bob performing an actual Z measurement. The cases for which $c \in \{3,4,5\}$ correspond to the actual X measurement rounds, while the case labelled by $c = 6$ is not useful for our analysis and is considered for normalisation purposes only.

Table 2. Emitted states $\left|\phi^{(c)}\right\rangle_B$ and associated probabilities p_c in the virtual protocol. The quantity $p_{a^{\text{virt}}_X}$ for $a \in \{0,1\}$ is the probability of Alice sending the virtual state $\left|\phi^{\text{virt}}_{a_X}\right\rangle_B$ and is given by equation (A6), while p_{γ_A} (p_{γ_B}) denotes the probability of Alice (Bob) selecting the basis $\gamma \in \{X,Z\}$ to prepare (measure) the quantum states.

c	$\left\|\phi^{(c)}\right\rangle_B$	p_c	Bob's basis
1	$\left\|\phi^{\text{virt}}_{0_X}\right\rangle_B$	$p_{0^{\text{virt}}_X} p_{Z_A} p_{Z_B}$	virtual X
2	$\left\|\phi^{\text{virt}}_{1_X}\right\rangle_B$	$p_{1^{\text{virt}}_X} p_{Z_A} p_{Z_B}$	virtual X
3	$\left\|\phi_{0_Z}\right\rangle_B$	$p_{Z_A} p_{X_B}/2$	X
4	$\left\|\phi_{1_Z}\right\rangle_B$	$p_{Z_A} p_{X_B}/2$	X
5	$\left\|\phi_{0_X}\right\rangle_B$	$p_{X_A} p_{X_B}$	X
6	$\left\|\phi_{0_X}\right\rangle_B$	$p_{X_A} p_{Z_B}$	Z

the fact that the operator associated to failed filtering for $\hat{Q}_\beta$ is indeed $\sqrt{\hat{M}^{\text{fail}_\beta}_{BT}}$. In this respect, the sifted key rounds are those where the filtering $\hat{Q}_Z$ is successful (note that Alice's measurements of her shield system are always successful). We summarise the two equivalent descriptions of Bob's POVMs in figure 8.

We conclude remarking that although our analysis applies to a system T of arbitrary dimension, for all practical purposes it might be beneficial to consider it to be finite [37]. In fact, Bob could, in principle, apply some mode-correction filtering at the entrance of his lab, effectively limiting the dimensionality of possible input modes. For example, when the system T models shifts in the time of arrival of the signals, one can consider a finite number of discrete shifts by introducing a Gaussian filtering operation at the entry of the lab [37]. Moreover, if only a partial characterisation of the efficiency operators is available, one should consider the worst case scenario minimising the SKR given by equation (13) over the possible missing entries of $\hat{F}_s{}^\dagger \hat{F}_s$, which might cause the problem to be intractable for a system T of infinite dimension. Finally, note that while we restrict our analysis to a single efficiency-affecting mode, this approach can be generalised in a

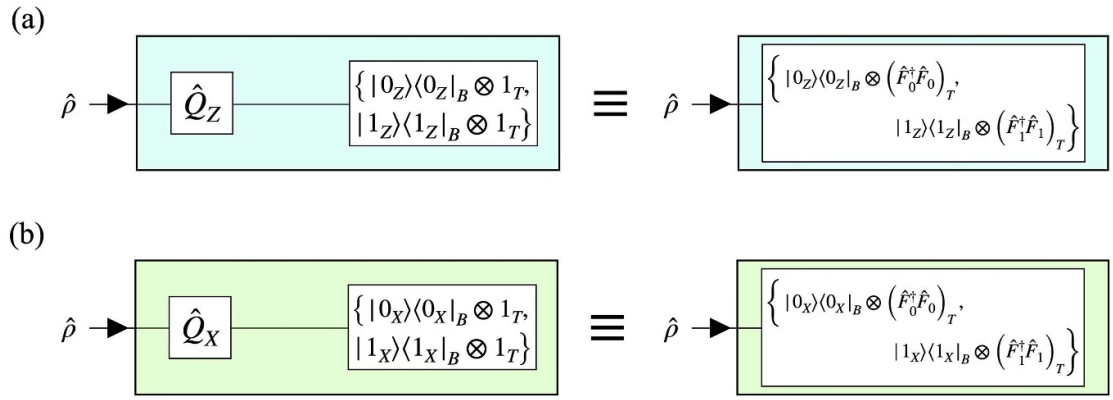


Figure 8. Bob's scheme for a successful measurement in (a) the Z basis and (b) the X basis. For each figure, Bob's POVM elements corresponding to a successful measurement outcome (right-hand side) can be equivalently described by a filter $\hat{Q}_\beta$, with $\beta \in \{X, Z\}$, which determines whether or not the states $\hat{\rho}$ coming from the channel trigger a detection, followed by projective measurements to assign the bit value (left-hand side). A failed measurement is equivalently described by the $\hat{M}_{BT}^{s_\beta}$ POVM element or the $\hat{Q}_\beta$ filter not succeeding.

straightforward way to a scenario with several efficiency-affecting modes, simply by considering multiple systems $T_1, \ldots, T_n$ and defining efficiency matrices $\hat{F}_s^\dagger \hat{F}_s$ for each of them.

Appendix B. Security against coherent attacks

In this appendix we provide the full security proof against coherent attacks. We do so by first developing an analytical description of the way Bob's outcomes for the actual signal states are affected by Eve's attack and by his measurement schemes (section B.1). From here, we extend the description to the case of virtual states, relating their statistics to those of the actual states (section B.2). We conclude the analysis by computing a lower bound on the SKR (section B.3) through an upper bound on the phase-error rate (section B.4). The conceptual map of our approach is depicted in figure 9.

B.1. Security analysis of the actual states

Let

$$|\Phi\rangle_{ABT} = \left|\varphi^{(<l)}\right\rangle_{ABT} \left|\varphi^{(l)}\right\rangle_{ABT} \left|\varphi^{(>l)}\right\rangle_{ABT}, \tag{B1}$$

denote the global state prepared by Alice during N rounds of the protocol, where $\left|\varphi^{(<l)}\right\rangle_{ABT}$ ($\left|\varphi^{(>l)}\right\rangle_{ABT}$) denotes the full set of states of the rounds that precede (follow) round l. The lth round state takes the form given by equation (A7).

For coherent attacks, the action of Eve is represented by a joint unitary operator $\hat{V}_{BTE}$ acting on all the transmitted systems BT, together with Eve's ancillary system E, resulting in a state $|\Psi\rangle$ given by

$$|\Psi\rangle = \hat{V}_{BTE} |\Phi\rangle_{ABT} |0\rangle_E = \sum_i \hat{E}_{BT}^{(i)} |\Phi\rangle_{ABT} |i\rangle_E. \tag{B2}$$

Let now

$$\hat{O}_{ABT}^{(l-1)} := \bigotimes_{u=1}^{l-1} \hat{M}_{ABT}^{c^u, s_\beta^u}, \tag{B3}$$

where $\hat{M}_{ABT}^{c^u, s_\beta^u} := |c\rangle\langle c|_{A_u} \otimes \hat{M}_{B_u T_u}^{s_\beta}$ is the Kraus operator associated to the measurement of the systems A, B and T at round u, yielding outcome c for the shield system and $s \in \{0, 1\}$ for Bob's measurement in the basis $\beta \in \{X, Z\}$. The joint state of systems A, B and T at round l conditioned on the previous observations is then given by

$$\hat{\rho}_{ABT}^{l|O^{(l-1)}} = \sum_i \mathrm{Tr}_{\bar{l}} \left[\hat{P}\left(\hat{O}_{ABT}^{(l-1)} \hat{E}_{BT}^{(i)} |\Phi\rangle_{ABT}\right)\right] / p^{(l)},$$

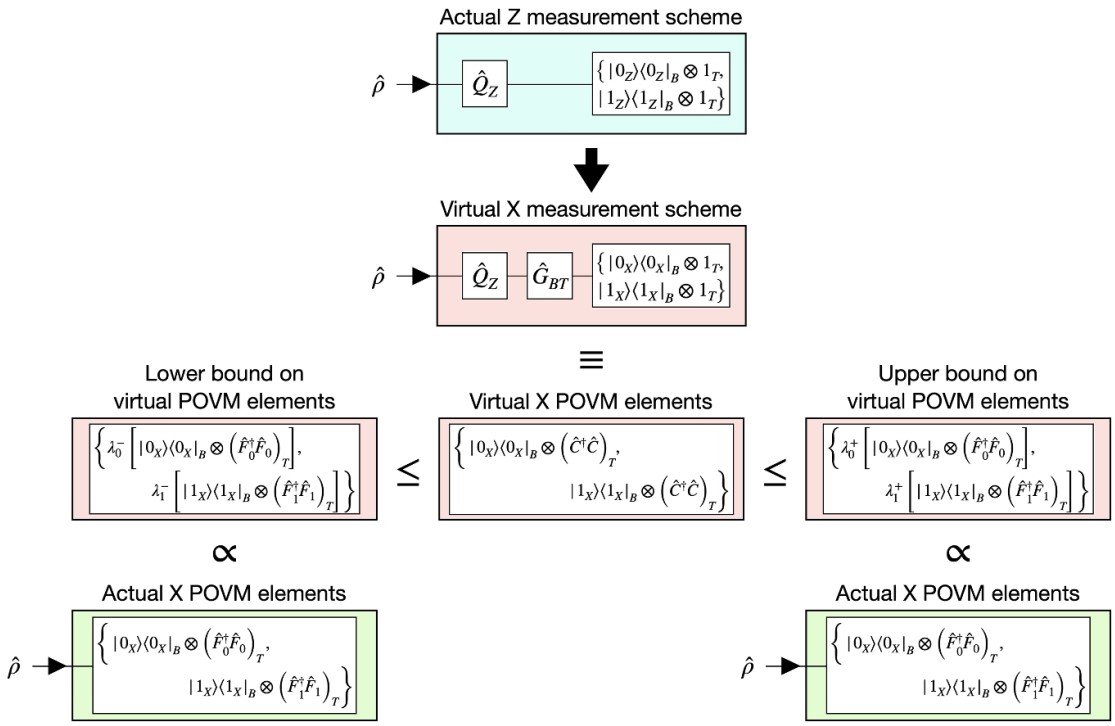


Figure 9. Workflow of the security proof provided in this paper. The boxes in this figure refer to either the actual measurements illustrated in figure 8, or the virtual measurement reported in figure 10. For the sifted key rounds, we consider a virtual framework where Bob's actual Z measurement is substituted by a virtual one. The latter is designed by first employing the same filter $\hat{Q}_Z$, such that the length of the sifted key in the actual and virtual schemes is preserved. Then, an additional virtual filter $\hat{G}_{BT}$ is applied, before a projective measurement in the X basis is performed. By properly choosing the virtual filter $\hat{G}_{BT}$, we can balance the DEM, such that the efficiency associated to Bob's measurements on system B is the same for every state of the system T. From here, we lower and upper bound these POVM operators so that each efficiency operator $\hat{F}_s{}^{\dagger}\hat{F}_s$ is coupled to the projector $|s_X\rangle\langle s_X|_B$ in the X basis, for $s \in \{0,1\}$. Crucially, these bound operators are now proportional to the measurements that Bob actually performs in the X basis. As a result, we can relate Bob's virtual measurement results to the experimental data.

$$p^{(l)} = \mathrm{Tr}\left[\sum_i \mathrm{Tr}_{\bar{l}}\left[\hat{P}\left(\hat{O}_{ABT}^{(l-1)}\hat{E}_{BT}^{(i)}|\Phi\rangle_{ABT}\right)\right]\right], \tag{B4}$$

where $\mathrm{Tr}_{\bar{l}}$ represents the trace over all systems but A, B and T at round l and $\hat{P}(|\psi\rangle) := |\psi\rangle\langle\psi|$. By letting $\{|\vec{x}_{<l}\rangle\}$ ($\{|\vec{x}_{>l}\rangle\}$) denote an orthonormal basis for the state of the rounds before (after) l, we can explicitly write the trace operator in equation (B4) to find

$$\begin{aligned}
\hat{\rho}_{ABT}^{l|O^{(l-1)}}\cdot p^{(l)} &= \sum_i \mathrm{Tr}_{\bar{l}}\left[\hat{P}\left(\hat{O}_{ABT}^{(l-1)}\hat{E}_{BT}^{(i)}|\Phi\rangle_{ABT}\right)\right] \\
&= \sum_i \sum_{\vec{x}_{<l}}\sum_{\vec{x}_{>l}} \langle\vec{x}_{<l}|\,\langle\vec{x}_{>l}|\hat{P}\left(\hat{O}_{ABT}^{(l-1)}\hat{E}_{BT}^{(i)}|\Phi\rangle_{ABT}\right)|\vec{x}_{<l}\rangle\,|\vec{x}_{>l}\rangle_{ABT} \\
&= \sum_i \sum_{\vec{x}_{<l},\vec{x}_{>l}} \hat{P}\left(\hat{A}_{i;BT|O^{(l-1)}}^{(\vec{x}_{<l},\vec{x}_{>l})}\left|\varphi^{(l)}\right\rangle_{ABT}\right) \\
&= \sum_i \sum_{\vec{x}_{<l},\vec{x}_{>l}} \hat{P}\left(\sum_c \sqrt{p_c}|c\rangle_A \hat{A}_{i;BT|O^{(l-1)}}^{(\vec{x}_{<l},\vec{x}_{>l})}\left|\phi^{(c)}\right\rangle_B |0\rangle_T\right),
\end{aligned} \tag{B5}$$

where we have defined

$$\hat{A}_{i;BT|O^{(l-1)}}^{(\vec{x}_{<l},\vec{x}_{>l})} := \langle\vec{x}_{<l}|\left\langle\vec{x}_{>l}\right|\hat{O}_{ABT}^{(l-1)}\hat{E}_{BT}^{(i)}\left|\varphi^{(<l)}\right\rangle_{ABT}\left|\varphi^{(>l)}\right\rangle_{ABT}. \tag{B6}$$

This operator acts jointly on the systems B and T at round l and can be decomposed as

$$\hat{A}_{i;BT|O^{(l-1)}}^{(\vec{x}_{<l},\vec{x}_{>l})} = \sum_k \hat{A}_{i,k;B|O^{(l-1)}}^{(\vec{x}_{<l},\vec{x}_{>l})} \otimes \hat{A}_{i,k;T|O^{(l-1)}}^{(\vec{x}_{<l},\vec{x}_{>l})} \tag{B7}$$

over the two systems. For further reference, we define the (unnormalised) action of the element $\hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,k;T|O^{(l-1)}}$ on the system T as

$$\left|\gamma^{(l,i,k)}\right\rangle_T := \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,k;T|O^{(l-1)}} |0\rangle_T, \tag{B8}$$

such that from equation (B5) it follows

$$\hat{\rho}^{l|O^{(l-1)}}_{ABT} = \frac{1}{p^{(l)}} \sum_i \sum_{\vec{x}_{<l},\vec{x}_{>l}} \hat{P}\left(\sum_{c,k} \sqrt{p_c} |c\rangle_A \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,k;B|O^{(l-1)}} \left|\phi^{(c)}\right\rangle_B \left|\gamma^{(l,i,k)}\right\rangle_T\right). \tag{B9}$$

We are interested in computing the joint probabilities $P_{s_X,c|O^{(l-1)}}$ of Bob obtaining outcome s_X at round l by measuring the system B in the X basis and Alice sending the cth state $\left|\phi^{(c)}\right\rangle_B$, conditioned on all the previous results. For the actual states measured in the X basis (that is, when $c \in \{3,4,5\}$), we have that

$$\begin{aligned}
P_{s_X,c|O^{(l-1)}} &= \mathrm{Tr}\left[\left(|c\rangle\langle c|_A \otimes \hat{M}^{s_X}_{BT}\right) \hat{\rho}^{l|O^{(l-1)}}_{ABT}\right] \\
&= \frac{p_c}{p^{(l)}} \sum_i \sum_{\vec{x}_{<l},\vec{x}_{>l}} \mathrm{Tr}\left[\hat{M}^{s_X}_{BT} \hat{P}\left(\sum_k \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,k;B|O^{(l-1)}} \left|\phi^{(c)}\right\rangle_B \left|\gamma^{(l,i,k)}\right\rangle_T\right)\right] \\
&= \frac{p_c}{p^{(l)}} \sum_{i,k,k'} \sum_{\vec{x}_{<l},\vec{x}_{>l}} \left\langle\gamma^{(l,i,k')}\right| \hat{F}_s{}^\dagger \hat{F}_s \left|\gamma^{(l,i,k)}\right\rangle_T \\
&\quad \times \mathrm{Tr}\left[\hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})\dagger}_{i,k';B|O^{(l-1)}} |s_X\rangle\langle s_X|_B \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,k;B|O^{(l-1)}} \hat{P}\left(\left|\phi^{(c)}\right\rangle_B\right)\right] \\
&= p_c \mathrm{Tr}\left[\hat{D}_{s_X|O^{(l-1)}} \hat{P}\left(\left|\phi^{(c)}\right\rangle_B\right)\right],
\end{aligned} \tag{B10}$$

where we have defined

$$\hat{D}_{s_X|O^{(l-1)}} := \frac{1}{p^{(l)}} \sum_{i,k,k'} \sum_{\vec{x}_{<l},\vec{x}_{>l}} \left\langle\gamma^{(l,i,k')}\right| \hat{F}_s{}^\dagger \hat{F}_s \left|\gamma^{(l,i,k)}\right\rangle_T \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})\dagger}_{i,k';B|O^{(l-1)}} |s_X\rangle\langle s_X|_B \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,k;B|O^{(l-1)}}. \tag{B11}$$

We can now proceed to decompose $\hat{P}\left(\left|\phi^{(c)}\right\rangle_B\right)$ in the Pauli basis. Let

$$(\hat{\sigma}_{\mathbb{1}}, \hat{\sigma}_X, \hat{\sigma}_Y, \hat{\sigma}_Z) = \left(\hat{\mathbb{1}}, \hat{X}, \hat{Y}, \hat{Z}\right) \tag{B12}$$

be the set of identity and Pauli matrices for system B. Then:

$$\hat{P}\left(\left|\phi^{(c)}\right\rangle_B\right) = \frac{1}{2} \sum_{\omega\in\Omega} W^{(c)}_\omega \hat{\sigma}_\omega, \tag{B13}$$

where $\Omega = \{\mathbb{1}, X, Y, Z\}$ and $\boldsymbol{W}^{(c)} := \left(1, V^{(c)}_X, V^{(c)}_Y, V^{(c)}_Z\right)^T$, being $V^{(c)}_t$ for $t \in \{X,Y,Z\}$ the entries of the Bloch vector of the state $\left|\phi^{(c)}\right\rangle_B$. Here, $W^{(c)}_{\mathbb{1}} = 1$. Also, note that we have $V^{(c)}_Y = 0\ \forall c$, as from Assumption (A1) all flawed states lay on the XZ-plane of the Bloch sphere. Substituting equation (B13) in equation (B10), one finds

$$P_{s_X,c|O^{(l-1)}} = p_c \sum_{\omega\in\Omega} W^{(c)}_\omega q_{s_X,\omega|O^{(l-1)}}, \tag{B14}$$

with

$$q_{s_X,\omega|O^{(l-1)}} := \frac{1}{2} \mathrm{Tr}\left[\hat{D}_{s_X|O^{(l-1)}} \hat{\sigma}_\omega\right]. \tag{B15}$$

By means of Kato's inequalities [70], we have that the sum of the probabilities in equation (B14) over all N rounds is asymptotically close to the number of occurrences of the corresponding events in the protocol, that is

$$\sum_{l=1}^N P_{s_X,c|O^{(l-1)}} = p_c \sum_{\omega\in\Omega} W^{(c)}_\omega \sum_{l=1}^N q_{s_X,\omega|O^{(l-1)}} \xrightarrow{N\to\infty} N_{s_X,c}, \tag{B16}$$

where $N_{s_X,c}$ is the number of times Alice sends the state $\left|\phi^{(c)}\right\rangle_B$ and Bob obtains the result s_X. From the idea of the LT protocol, as long as the vectors $\{\vec{W}^{(c)}\}_{c\in\{3,4,5\}}$ of the flawed quantum states are linearly independent, inverting the set of equations provided by equation (B16) for $c \in \{3,4,5\}$ allows to estimate the values of the terms $\sum_{l=1}^{N} q_{s_X,\omega|O^{(l-1)}}$ for $\omega \in \{\mathbb{1}, X, Z\}$ from the experimental data [49]. This corresponds to the result in equation (8), where $\forall\omega$ we define

$$\tilde{q}_{s_X,\omega} := \lim_{N\to\infty} \frac{1}{N} \sum_{l=1}^{N} q_{s_X,\omega|O^{(l-1)}}, \tag{B17}$$

and consider in the asymptotic limit

$$p_{s_X,c} := \lim_{N\to\infty} \frac{N_{s_X,c}}{N}. \tag{B18}$$

B.2. Security analysis of the virtual states

In the complementarity framework, the phase-error rate can be computed once we find the errors that Bob encounters in predicting Alice's virtual X outcomes for the states they use to produce the sifted key. Crucially, due to the DEM, the probability of successful detection in the Z or X basis for Bob is not the same. Therefore, to balance statistics, at round l we must consider the state going through the Z basis filter in equation (A8), namely

$$\hat{Q}_Z \hat{\rho}_{ABT}^{l|O^{(l-1)}} \hat{Q}_Z^\dagger. \tag{B19}$$

See figure 9 for reference.

To predict Alice's virtual X outcomes, Bob is allowed to apply any virtual filter $\hat{G}_{BT}$ on the above states. The goal is to design a virtual filter that allows him to rely on the information available from the experimental data. Ideally, the best option would be a virtual filter satisfying $\hat{G}_{BT}\hat{Q}_Z = \hat{Q}_X$. This would imply that for all events for which a conclusive outcome can be asserted in the Z basis, we can obtain a virtual X measurement conclusive event as well, which we can relate to the actual statistics in the X basis that Bob observes in his experiment. Crucially, due to the DEM this is not possible.

In this paper we adopt the filter proposed in [37], which is given by

$$\hat{G}_{BT} = |0_Z\rangle\langle 0_Z|_B \otimes \hat{C}\hat{F}_0^{-1} + |1_Z\rangle\langle 1_Z|_B \otimes \hat{C}\hat{F}_1^{-1}, \tag{B20}$$

followed by a projective measurement on $|s_X\rangle\langle s_X|_B \otimes \hat{\mathbb{1}}_T$. This corresponds to the definition of the following virtual POVMs acting on the state incoming from the channel

$$\hat{M}_{BT}^{s_X,\text{virt}} = \hat{Q}_Z^\dagger \hat{G}_{BT}^\dagger \left(|s_X\rangle\langle s_X|_B \otimes \hat{\mathbb{1}}_T\right) \hat{G}_{BT}\hat{Q}_Z. \tag{B21}$$

Importantly, the $\hat{C}$ matrix is chosen so to guarantee that $\hat{G}_{BT}$ is a valid filtering operation. Moreover, note that

$$\hat{G}_{BT}\hat{Q}_Z = \hat{\mathbb{1}}_B \otimes \hat{C}. \tag{B22}$$

This measurement scheme is depicted in figure 10.

At round l, if the virtual filtering is successful, the joint probability of Alice sending the virtual state $\left|\phi^{(c)}\right\rangle_B$ for $c \in \{1,2\}$ and Bob obtaining s_X (in the virtual scheme) for rounds where he actually measured in the Z basis, conditioned on all the previous results, is given by

$$\begin{aligned} P^{\text{virt}}_{s_X,c|O^{(l-1)}} &= \text{Tr}\left[\left(|c\rangle\langle c|_A \otimes \hat{M}_{BT}^{s_X,\text{virt}}\right)\hat{\rho}_{ABT}^{l|O^{(l-1)}}\right] \\ &= \text{Tr}\left[\left(|c\rangle\langle c|_A \otimes |s_X\rangle\langle s_X|_B \otimes \hat{C}^\dagger\hat{C}\right)\hat{\rho}_{ABT}^{l|O^{(l-1)}}\right] \\ &= p_c \text{Tr}\left[\hat{D}^{\text{virt}}_{s_X|O^{(l-1)}}\hat{P}\left(\left|\phi^{(c)}\right\rangle_B\right)\right] \\ &= p_c \sum_{\omega\in\Omega} W_\omega^{(c)} q^{\text{virt}}_{s_X,\omega|O^{(l-1)}}, \end{aligned} \tag{B23}$$

where we have defined

$$\hat{D}^{\text{virt}}_{s_X|O^{(l-1)}} := \frac{1}{p^{(l)}} \sum_{i,k,k'} \sum_{\vec{x}_{<l},\vec{x}_{>l}} \left\langle \gamma^{(l,i,k')}\middle|\hat{C}^\dagger\hat{C}\middle|\gamma^{(l,i,k)}\right\rangle_T \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})\dagger}_{i,k';B|O^{(l-1)}} |s_X\rangle\langle s_X|_B \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,k;B|O^{(l-1)}}, \tag{B24}$$

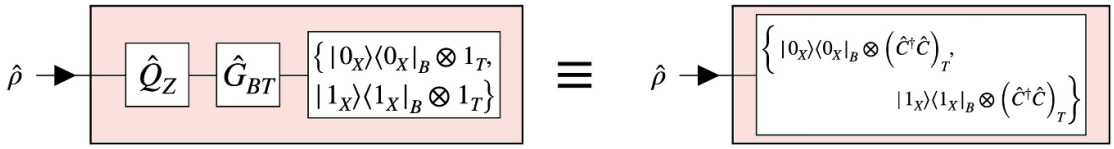


Figure 10. Bob's scheme for a successful measurement in the virtual scheme. Bob is allowed to perform any virtual operation on the incoming states in order to maximise his ability to guess Alice's virtual X outcome. Here, this corresponds to apply the filter $\hat{Q}_Z$ to make sure the total number of detections in the Z basis for the virtual and actual protocols are the same, and then an additional filter $\hat{G}_{BT}$, followed by projective measurements. A failed measurement in the virtual protocol is equivalently described by the POVM element $\hat{\mathbb{1}} - \hat{M}_{BT}^{0_X,\text{virt}} - \hat{M}_{BT}^{1_X,\text{virt}}$ or, equivalently, the total filter $\hat{G}_{BT}\hat{Q}_Z$ not succeeding.

and

$$q^{\text{virt}}_{s_X,\omega|O^{(l-1)}} = \frac{1}{2}\text{Tr}\left[\hat{D}^{\text{virt}}_{s_X|O^{(l-1)}}\hat{\sigma}_\omega\right]. \tag{B25}$$

As shown in appendix C, once we consider the sum over all rounds we can rewrite these terms in a more convenient form given by

$$\sum_{l=1}^{N} P^{\text{virt}}_{s_X,c|O^{(l-1)}} = p_c \sum_{\omega\in\Omega} W^{(c)}_\omega \sum_{l=1}^{N} q^{\text{virt}}_{s_X,\omega|O^{(l-1)}} = \frac{p_c}{2}\sum_{\omega\in\Omega} W^{(c)}_\omega \text{Tr}\left[\hat{\rho}_E\left(\hat{T}_{s_X,\omega}\otimes \hat{C}^\dagger\hat{C}\right)\right], \tag{B26}$$

where $\hat{\rho}_E$ is a quantum state under full control of Eve that encodes all the information of her attack (i.e. the terms $\hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i;BT|O^{(l-1)}}$ in equation (B6)) and, as such, its size depends on the number of rounds N. On the other hand, $\hat{T}_{s_X,\omega}$ is a 4×4 matrix whose analytic form is reported in equations (C9)–(C11). In appendix C we also discuss how for the terms $q_{s_X,\omega|O^{(l-1)}}$ in equation (B15) it holds the similar relation

$$\sum_{l=1}^{N} q_{s_X,\omega|O^{(l-1)}} = \frac{1}{2}\text{Tr}\left[\hat{\rho}_E\left(\hat{T}_{s_X,\omega}\otimes \hat{F}_s{}^\dagger\hat{F}_s\right)\right]. \tag{B27}$$

The combination of the results in equations (B26) and (B27) allows to bound the statistics of the virtual X measurement in the virtual protocol, given knowledge of the generalised efficiency operators $\hat{F}_s{}^\dagger\hat{F}_s$ and the terms $q_{s_X,\omega|O^{(l-1)}}$ learned from the LT approach. This step is illustrated in section B.4.

For application in the next section and for better clarity, let us define from equation (B23)

$$P^{(l)}_{s^v_X,0^v_X} := P^{\text{virt}}_{s_X,c=1|O^{(l-1)}}, \quad P^{(l)}_{s^v_X,1^v_X} := P^{\text{virt}}_{s_X,c=2|O^{(l-1)}}, \tag{B28}$$

such that $P^{(l)}_{s^v_X,a^v_X}$ denotes the joint probability at round l of Bob and Alice respectively obtaining an outcome s and a in the virtual measurement scheme, conditioned on all the previous results.

B.3. Computing the SKR

Formally, in the asymptotic limit, the probability of being in a sifted key round and the probability of having a bit error in the Z basis are respectively given by

$$p^{\text{sift}}_Z = \lim_{N\to\infty}\frac{1}{N}\sum_{a,s=0}^{1} N_{s_Z,a_Z}, \qquad p^{\text{err}}_Z := \lim_{N\to\infty}\frac{1}{N}\sum_{a\neq s} N_{s_Z,a_Z}, \tag{B29}$$

where N_{s_Z,a_Z} indicates the number of occurrences in which Bob obtains a Z measurement outcome s and Alice prepares the state $|\phi_{a_Z}\rangle_B$. Note that both quantities are directly estimated by Alice in the protocol (see section 3), and that the bit error rate can be directly computed from their ratio as indicated in equation (15).

As discussed in appendix A.2, the rounds with a detection in the Z basis are the ones for which the filter $\hat{Q}_Z$ in equation (A8) is successful. For these rounds, in the virtual protocol Bob applies the virtual filter $\hat{G}_{BT}$ provided in equation (B20). The average of the probabilities of Bob's virtual X measurement being successful (which are conditional on Alice and Bob's measurement outcomes in the previous rounds of the virtual protocol and include the probability of being in a sifted key round) is given by

$$p^{\text{virt}}_X := \lim_{N\to\infty}\frac{1}{N}\sum_{a,s=0}^{1} N_{s^v_X,a^v_X}, \tag{B30}$$

where $N_{s_X^v,a_X^v}$ indicates the number of occurrences in which Bob obtains a virtual X measurement outcome s and Alice prepares the state $\left|\phi_{a_X}^{\text{virt}}\right\rangle_B$. Crucially, this is an average probability because Bob's virtual X measurement consist of filtering operations, whose success probability is, in all generality, different at every round, since it depends on the specific states that the filter acts on.

With similar reasoning, the average probability of having a bit error in Bob's virtual X measurement is given by

$$p_{X^{\text{virt}}}^{\text{err}} := \lim_{N\to\infty} \frac{1}{N} \sum_{a\neq s} N_{s_X^v,a_X^v}. \tag{B31}$$

We note that the terms on the right-hand side of equations (B30) and (B31) can be estimated as the sum over the round index l of the quantities $P^{(l)}_{s_X^v,a_X^v}$ in equation (B28) for $N\to\infty$, thanks to Kato's inequality [70]. As a result, we can define in the asymptotic regime the fraction of sifted key rounds in which Bob's virtual X measurement is successful as

$$r_X^{\text{virt}} := \frac{p_X^{\text{virt}}}{p_Z^{\text{sift}}} = \frac{1}{p_Z^{\text{sift}}} \lim_{N\to\infty} \frac{1}{N} \left[\sum_{l=1}^{N} \left(P^{(l)}_{0_X^v,0_X^v} + P^{(l)}_{1_X^v,0_X^v} + P^{(l)}_{0_X^v,1_X^v} + P^{(l)}_{1_X^v,1_X^v}\right)\right]. \tag{B32}$$

Finally, we compute the phase-error rate e_p, which is the probability of Bob making an error in the guess of Alice's virtual X outcome for the sifted rounds. Following the same argument of equation (B32), in the asymptotic limit we have that

$$e_p := \frac{p_{X^{\text{virt}}}^{\text{err}}}{p_X^{\text{virt}}} = \frac{\lim_{N\to\infty} \frac{1}{N} \sum_{l=1}^{N} \left(P^{(l)}_{0_X^v,1_X^v} + P^{(l)}_{1_X^v,0_X^v}\right)}{\lim_{N\to\infty} \frac{1}{N} \sum_{l=1}^{N} \left(P^{(l)}_{0_X^v,0_X^v} + P^{(l)}_{1_X^v,0_X^v} + P^{(l)}_{0_X^v,1_X^v} + P^{(l)}_{1_X^v,1_X^v}\right)}. \tag{B33}$$

According to Koashi's security proof [62], these quantities allow Alice and Bob to compute how many sifted bits they must sacrifice for the sake of privacy amplification. In detail, to remove any residual information shared with Eve, Alice and Bob must perform hashing on their sifted keys for all the rounds in which Bob's virtual filter $\hat{G}_{BT}$ was not successful (note that the average probability of the virtual filter failing is given by $p_Z^{\text{sift}} - p_X^{\text{virt}}$), plus additional rounds to counteract the erroneous estimates of Bob. Over N rounds of the protocol, this last term is given by $Np_X^{\text{virt}} h_2\left(e_p\right)$, where $h_2\left(x\right)$ denotes the binary entropy, and the total number of hashing rounds required for privacy amplification is given by

$$M_{\text{PA}} = Np_Z^{\text{sift}}\left(1 - r_X^{\text{virt}}\right) + Np_Z^{\text{sift}} r_X^{\text{virt}} h_2\left(e_p\right). \tag{B34}$$

Moreover, Alice and Bob must sacrifice additional

$$M_{\text{EC}} = fNp_Z^{\text{sift}} h_2\left(e_b\right) \tag{B35}$$

sifted key bits to perform error correction (EC), with an EC code of efficiency f. Putting all considerations together, the asymptotic SKR per signal sent can be retrieved to be

$$R \geqslant \lim_{N\to\infty} \frac{1}{N}\left(Np_Z^{\text{sift}} - M_{\text{PA}} - M_{\text{EC}}\right) \tag{B36}$$

$$= p_Z^{\text{sift}}\left[r_X^{\text{virt}}\left(1 - h_2\left(e_p\right)\right) - fh_2\left(e_b\right)\right]. \tag{B37}$$

By considering a lower bound on r_X^{virt} and an upper bound on e_p, equation (13) follows naturally.

Crucially, the terms $P^{(l)}_{s_X^v,a_X^v}$ in equations (B32) and (B33) depend on the choice of the operator $\hat{C}$ in the definition of the virtual filter. As the optimal choice of $\hat{C}$ might be subject to the specifics of the channel, in this work we consider for simplicity the operator $\hat{C}$ originally proposed in [37], which has been obtained optimising the noiseless case (that is, without SPFs and attacks on the B system). In the following section we show how this choice for $\hat{C}$ allows to directly bound the phase-error rate given the experimental data and a characterisation of the devices efficiency operators.

B.4. Bounding the phase-error rate

As illustrated in figure 9, to relate the phase-error rate to the statistics of the actual X basis measurements we must find lower and upper bounds on the operator $\hat{C}^\dagger\hat{C}$ in the form given by equation (12). One viable option to do so is to employ semidefinite programming, as discussed in section 4. Alternatively, here we compute the analytical bounds provided by equation (20).

From equations (9)–(11), we define $D_{\min}$ ($D_{\max}$) as the minimum (maximum) eigenvalue of $\hat{D}$. It follows that the minimum (maximum) eigenvalue of $\hat{C}_1{}^\dagger\hat{C}_1$ is $\eta_{\min} := \min\left(D_{\max}^{-1}, 1\right)$ ($\eta_{\max} := \min\left(D_{\min}^{-1}, 1\right)$). Therefore, we have that

$$\eta_{\min}\hat{\mathbb{1}} + \hat{C}' = \hat{C}_1{}^\dagger\hat{C}_1 = \eta_{\max}\hat{\mathbb{1}} - \hat{C}'', \tag{B38}$$

where $\hat{C}'$ and $\hat{C}''$ are positive semi-definite diagonal matrices. Therefore

$$\begin{aligned}\hat{C}^\dagger\hat{C} &= \hat{F}_0^\dagger\hat{U}\hat{C}_1{}^\dagger\hat{C}_1\hat{U}^\dagger\hat{F}_0\\ &= \eta_{\min}\hat{F}_0{}^\dagger\hat{F}_0 + \hat{F}_0^\dagger\hat{U}\hat{C}'\hat{U}^\dagger\hat{F}_0\\ &\geqslant \eta_{\min}\hat{F}_0{}^\dagger\hat{F}_0,\end{aligned} \tag{B39}$$

where the inequality holds because the term $\hat{F}_0^\dagger\hat{U}\hat{C}'\hat{U}^\dagger\hat{F}_0$ is positive semi-definite. Similarly, one finds

$$\hat{C}^\dagger\hat{C} \leqslant \eta_{\max}\hat{F}_0{}^\dagger\hat{F}_0. \tag{B40}$$

Moreover, from equation (9) we have that

$$\hat{F}_1{}^\dagger\hat{F}_1 = \hat{F}_0^\dagger\hat{U}\hat{D}^{-1}\hat{U}^\dagger\hat{F}_0, \tag{B41}$$

which is in the same form as the first line of equation (B39), with the substitutions $\hat{C}^\dagger\hat{C} \to \hat{F}_1{}^\dagger\hat{F}_1$ and $\hat{C}_1{}^\dagger\hat{C}_1 \to \hat{D}^{-1}$. By applying the same reasoning, we obtain

$$\frac{1}{D_{\max}}\hat{F}_0{}^\dagger\hat{F}_0 \leqslant \hat{F}_1{}^\dagger\hat{F}_1 \leqslant \frac{1}{D_{\min}}\hat{F}_0{}^\dagger\hat{F}_0, \tag{B42}$$

which can be inverted to find bounds on $\hat{F}_0{}^\dagger\hat{F}_0$ in terms of $\hat{F}_1{}^\dagger\hat{F}_1$. The combination of the results of equations (B39), (B40) and (B42) yields the analytical bounds in equation (20).

Now, bounds in equation (12) are defined for the operator $\hat{C}^\dagger\hat{C} \in \mathcal{H}_T$ acting on the T system. Nevertheless, it is straightforward to generalise them to operators in the form

$$\hat{\Pi} \otimes \hat{C}^\dagger\hat{C} \in \mathcal{H}_4 \otimes \mathcal{H}_T, \tag{B43}$$

where $\hat{\Pi}$ is a 4×4 projector. As expectation values for projective measurements are bounded in $[0, 1]$, one finds

$$\lambda_s^-\left(\hat{\Pi} \otimes \hat{F}_s{}^\dagger\hat{F}_s\right) \leqslant \left(\hat{\Pi} \otimes \hat{C}^\dagger\hat{C}\right) \leqslant \lambda_s^+\left(\hat{\Pi} \otimes \hat{F}_s{}^\dagger\hat{F}_s\right). \tag{B44}$$

This is particularly relevant since the terms $\hat{T}_{s_X,\omega}$ in equation (B26) are a linear combination of projectors, as we show in appendix C. By paying attention to the sign these projectors come with in the definition of $\hat{T}_{s_X,\omega}$, one can conveniently apply upper and lower bounds. For example, consider the operator

$$\hat{T}_{0_X,X} = \tilde{X}_{++} - \tilde{X}_{-+}, \tag{B45}$$

where $\tilde{X}_{++}$ and $\tilde{X}_{-+}$ are projectors (see equation (C6)). It is possible to upper bound $\hat{T}_{0_X,X}$ by upper bounding its positive component and lower bounding its negative component as

$$\begin{aligned}\hat{T}_{0_X,\hat{X}} \otimes \hat{C}^\dagger\hat{C} &= \tilde{X}_{++} \otimes \hat{C}^\dagger\hat{C} - \tilde{X}_{-+} \otimes \hat{C}^\dagger\hat{C}\\ &\leqslant \lambda_0^+\left(\tilde{X}_{++} \otimes \hat{F}_0{}^\dagger\hat{F}_0\right) - \lambda_0^-\left(\tilde{X}_{-+} \otimes \hat{F}_0{}^\dagger\hat{F}_0\right).\end{aligned} \tag{B46}$$

From equation (B46), one directly finds

$$\begin{aligned}\sum_{l=1}^{N} q^{\text{virt}}_{0_X,X|O^{(l-1)}} &= \frac{1}{2}\text{Tr}\left[\hat{\rho}_E\left(\hat{T}_{0_X,X}\otimes\hat{C}^\dagger\hat{C}\right)\right]\\ &\leqslant \frac{\lambda_0^+}{2}\text{Tr}\left[\hat{\rho}_E\left(\tilde{X}_{++}\otimes\hat{F}_0{}^\dagger\hat{F}_0\right)\right]-\frac{\lambda_0^-}{2}\text{Tr}\left[\hat{\rho}_E\left(\tilde{X}_{-+}\otimes\hat{F}_0{}^\dagger\hat{F}_0\right)\right]\\ &= \frac{\lambda_0^+}{2}\text{Tr}\left[\hat{\rho}_E\left(\frac{\hat{T}_{0_X,\mathbb{1}}+\hat{T}_{0_X,X}}{2}\otimes\hat{F}_0{}^\dagger\hat{F}_0\right)\right]\\ &\quad-\frac{\lambda_0^-}{2}\text{Tr}\left[\hat{\rho}_E\left(\frac{\hat{T}_{0_X,\mathbb{1}}-\hat{T}_{0_X,X}}{2}\otimes\hat{F}_0{}^\dagger\hat{F}_0\right)\right]\\ &= \frac{\lambda_0^++\lambda_0^-}{4}\text{Tr}\left[\hat{\rho}_E\left(\hat{T}_{0_X,X}\otimes\hat{F}_0{}^\dagger\hat{F}_0\right)\right]\\ &\quad+\frac{\lambda_0^+-\lambda_0^-}{4}\text{Tr}\left[\hat{\rho}_E\left(\hat{T}_{0_X,\mathbb{1}}\otimes\hat{F}_0{}^\dagger\hat{F}_0\right)\right]\\ &= \frac{\lambda_0^++\lambda_0^-}{2}\sum_{l=1}^{N} q_{0_X,X|O^{(l-1)}}+\frac{\lambda_0^+-\lambda_0^-}{2}\sum_{l=1}^{N} q_{0_X,\mathbb{1}|O^{(l-1)}}\,.\end{aligned}\tag{B47}$$

Reasoning in a similar way, we obtain that for $s\in\{0,1\}$ it holds

$$\lambda_s^-\sum_{l=1}^{N} q_{s_X,\mathbb{1}|O^{(l-1)}}\leqslant\sum_{l=1}^{N} q^{\text{virt}}_{s_X,\mathbb{1}|O^{(l-1)}}\leqslant\lambda_s^+\sum_{l=1}^{N} q_{s_X,\mathbb{1}|O^{(l-1)}}\,,\tag{B48}$$

and

$$\begin{aligned}&\frac{\lambda_s^++\lambda_s^-}{2}\sum_{l=1}^{N} q_{s_X,X|O^{(l-1)}}-\frac{\lambda_s^+-\lambda_s^-}{2}\sum_{l=1}^{N} q_{s_X,\mathbb{1}|O^{(l-1)}}\\ &\leqslant\sum_{l=1}^{N} q^{\text{virt}}_{s_X,X|O^{(l-1)}}\leqslant\frac{\lambda_s^++\lambda_s^-}{2}\sum_{l=1}^{N} q_{s_X,X|O^{(l-1)}}+\frac{\lambda_s^+-\lambda_s^-}{2}\sum_{l=1}^{N} q_{s_X,\mathbb{1}|O^{(l-1)}}\,.\end{aligned}\tag{B49}$$

Note that for detectors with equal efficiencies, $\hat{F}_0{}^\dagger\hat{F}_0=\hat{F}_1{}^\dagger\hat{F}_1\implies\hat{D}=\hat{\mathbb{1}}$, hence $\lambda_s^\pm=1$ and the sum over the virtual terms $q^{\text{virt}}_{s_X,\omega|O^{(l-1)}}$ is the same as in the actual X measurement. As a result, we are back to the scenario of the original LT protocol and the phase-error rate is zero, as expected [49]. Moreover, in the general case the phase-error rate given by equation (B33) can be directly upper bounded in a LT fashion, given the results of equations (B48) and (B49). In fact, recalling the values of p_1 and p_2 from table 2, we have that

$$\begin{aligned}\sum_{l=1}^{N}\left(P^{(l)}_{0_X^v,1_X^v}+P^{(l)}_{1_X^v,0_X^v}\right) &= p_{1_X^{\text{virt}}}p_{Z_A}p_{Z_B}\sum_{l=1}^{N}\left(q^{\text{virt}}_{0_X,\hat{\mathbb{1}}|O^{(l-1)}}-q^{\text{virt}}_{0_X,X|O^{(l-1)}}\right)\\ &\quad+p_{0_X^{\text{virt}}}p_{Z_A}p_{Z_B}\sum_{l=1}^{N}\left(q^{\text{virt}}_{1_X,\hat{\mathbb{1}}|O^{(l-1)}}+q^{\text{virt}}_{1_X,X|O^{(l-1)}}\right)\\ &\leqslant p_{1_X^{\text{virt}}}p_{Z_A}p_{Z_B}\sum_{l=1}^{N}\left(\frac{3\lambda_0^+-\lambda_0^-}{2}q_{0_X,\hat{\mathbb{1}}|O^{(l-1)}}-\frac{\lambda_0^++\lambda_0^-}{2}q_{0_X,X|O^{(l-1)}}\right)\\ &\quad+p_{0_X^{\text{virt}}}p_{Z_A}p_{Z_B}\sum_{l=1}^{N}\left(\frac{3\lambda_1^+-\lambda_1^-}{2}q_{1_X,\hat{\mathbb{1}}|O^{(l-1)}}+\frac{\lambda_1^++\lambda_1^-}{2}q_{1_X,X|O^{(l-1)}}\right).\end{aligned}\tag{B50}$$

Similarly, we have that

$$\begin{aligned}&\sum_{l=1}^{N}\left(P^{(l)}_{0_X^v,1_X^v}+P^{(l)}_{1_X^v,1_X^v}+P^{(l)}_{0_X^v,0_X^v}+P^{(l)}_{1_X^v,0_X^v}\right)\\ &\quad=p_{1_X^{\text{virt}}}p_{Z_A}p_{Z_B}\sum_{l=1}^{N}\left(q^{\text{virt}}_{0_X,\hat{\mathbb{1}}|O^{(l-1)}}-q^{\text{virt}}_{0_X,X|O^{(l-1)}}+q^{\text{virt}}_{1_X,\hat{\mathbb{1}}|O^{(l-1)}}-q^{\text{virt}}_{1_X,X|O^{(l-1)}}\right)\end{aligned}$$

$$
\begin{aligned}
&+ p_{0_X^{\text{virt}}} p_{Z_A} p_{Z_B} \sum_{l=1}^{N} \left(q^{\text{virt}}_{0_X,\hat{\mathbb{1}}|O^{(l-1)}} + q^{\text{virt}}_{0_X,X|O^{(l-1)}} + q^{\text{virt}}_{1_X,\hat{\mathbb{1}}|O^{(l-1)}} + q^{\text{virt}}_{1_X,X|O^{(l-1)}} \right) \\
&\geqslant p_{1_X^{\text{virt}}} p_{Z_A} p_{Z_B} \sum_{l=1}^{N} \left(-\frac{\lambda_0^+ - 3\lambda_0^-}{2} q_{0_X,\hat{\mathbb{1}}|O^{(l-1)}} - \frac{\lambda_0^+ + \lambda_0^-}{2} q_{0_X,X|O^{(l-1)}} \right) \\
&+ p_{1_X^{\text{virt}}} p_{Z_A} p_{Z_B} \sum_{l=1}^{N} \left(-\frac{\lambda_1^+ - 3\lambda_1^-}{2} q_{1_X,\hat{\mathbb{1}}|O^{(l-1)}} - \frac{\lambda_1^+ + \lambda_1^-}{2} q_{1_X,X|O^{(l-1)}} \right) \\
&+ p_{0_X^{\text{virt}}} p_{Z_A} p_{Z_B} \sum_{l=1}^{N} \left(-\frac{\lambda_0^+ - 3\lambda_0^-}{2} q_{0_X,\hat{\mathbb{1}}|O^{(l-1)}} + \frac{\lambda_0^+ + \lambda_0^-}{2} q_{0_X,X|O^{(l-1)}} \right), \\
&+ p_{0_X^{\text{virt}}} p_{Z_A} p_{Z_B} \sum_{l=1}^{N} \left(-\frac{\lambda_1^+ - 3\lambda_1^-}{2} q_{1_X,\hat{\mathbb{1}}|O^{(l-1)}} + \frac{\lambda_1^+ + \lambda_1^-}{2} q_{1_X,X|O^{(l-1)}} \right), \\
&= p_{Z_A} p_{Z_B} \sum_{l=1}^{N} \left[-\frac{\lambda_0^+ - 3\lambda_0^-}{2} q_{0_X,\hat{\mathbb{1}}|O^{(l-1)}} - \frac{\lambda_1^+ - 3\lambda_1^-}{2} q_{1_X,\hat{\mathbb{1}}|O^{(l-1)}} + \right. \\
&\left. + \langle \phi_{0_Z} | \phi_{1_Z} \rangle \left(\frac{\lambda_0^+ + \lambda_0^-}{2} q_{0_X,X|O^{(l-1)}} + \frac{\lambda_1^+ + \lambda_1^-}{2} q_{1_X,X|O^{(l-1)}} \right) \right].
\end{aligned} \tag{B51}
$$

Note that in the last passage we retrieved the explicit form of the probability of sending the virtual states in equation (A6).

By dividing by N and taking the limit $N \to \infty$ of equations (B50) and (B51), and combining with the results of equation (B17) and equations (B30) and (B31), we can find the bounds on p_X^{virt} and $p_{X^{\text{virt}}}^{\text{err}}$ reported in equations (16)–(18). From here, the bounds $r_X^{\text{virt,L}}$ and e_p^U in equations (17) and (18) follow. Importantly, all quantities involved are known and include SPFs ($\langle \phi_{0_Z} | \phi_{1_Z} \rangle \neq 0$), DEM (in the values of the parameters $\lambda_s^{\pm}$ for $s \in \{0,1\}$) and the action of the channel (in the terms $q_{s_X,\omega|O^{(l-1)}}$).

Appendix C. Derivation of equation (B26)

Consider the following expansions of operators on the system B in terms of the Pauli basis. We have

$$
|s_X\rangle\langle s_X|_B = \frac{1}{2}\left(\hat{\mathbb{1}} + (-1)^s \hat{X}\right), \tag{C1}
$$

$$
\hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,k;B|O_{l-1}} = a_0^{(l,i,k)} \hat{\mathbb{1}} + a_1^{(l,i,k)} \hat{X} + i a_2^{(l,i,k)} \hat{Y} + a_3^{(l,i,k)} \hat{Z}, \tag{C2}
$$

$$
\hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})\dagger}_{i,k';B|O_{l-1}} = a_0^{(l,i,k')*} \hat{\mathbb{1}} + a_1^{(l,i,k')*} \hat{X} - i a_2^{(l,i,k')*} \hat{Y} + a_3^{(l,i,k')*} \hat{Z}. \tag{C3}
$$

In the following, let $a_t^{(l,i,k)} \equiv a_t$ and $a_t^{(l,i,k')*} \equiv a'^*_t$ with $t \in \{0,1,2,3\}$ for ease of notation.

By exploiting the properties of the trace of the product of Pauli matrices, with the notation introduced in equation (B12) we notice that

$$
\text{Tr}\left[\hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})\dagger}_{i,k';B|O_{l-1}} |s_X\rangle\langle s_X|_B \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,k;B|O_{l-1}} \hat{\sigma}_\omega \right] = E^{(l,i,k,k')}_{\mathbb{1},\omega} + (-1)^s E^{(l,i,k,k')}_{X,\omega}, \tag{C4}
$$

where $\omega \in \{\mathbb{1}, X, Z\}$ and

$$
\begin{aligned}
E^{(l,i,k,k')}_{\mathbb{1},\mathbb{1}} &= a'^*_0 a_0 + a'^*_1 a_1 + a'^*_2 a_2 + a'^*_3 a_3, \\
E^{(l,i,k,k')}_{\mathbb{1},X} &= a'^*_1 a_0 + a'^*_0 a_1 + a'^*_2 a_3 + a'^*_3 a_2, \\
E^{(l,i,k,k')}_{\mathbb{1},Z} &= a'^*_3 a_0 + a'^*_0 a_3 - a'^*_1 a_2 - a'^*_2 a_1, \\
E^{(l,i,k,k')}_{X,\mathbb{1}} &= a'^*_1 a_0 + a'^*_0 a_1 - a'^*_3 a_2 - a'^*_2 a_3, \\
E^{(l,i,k,k')}_{X,X} &= a'^*_0 a_0 + a'^*_1 a_1 - a'^*_2 a_2 - a'^*_3 a_3, \\
E^{(l,i,k,k')}_{X,Z} &= a'^*_3 a_1 + a'^*_1 a_3 - a'^*_0 a_2 - a'^*_2 a_0.
\end{aligned} \tag{C5}
$$

Now, let

$$\begin{aligned}
\tilde{Z}_{00} &:= \hat{P}\left([1,0,0,1]^{\dagger}\right)/2, & \tilde{Z}_{01} &:= \hat{P}\left([0,1,-1,0]^{\dagger}\right)/2,\\
\tilde{Z}_{10} &:= \hat{P}\left([0,1,1,0]^{\dagger}\right)/2, & \tilde{Z}_{11} &:= \hat{P}\left([1,0,0,-1]^{\dagger}\right)/2,\\
\tilde{X}_{++} &:= \hat{P}\left([1,1,0,0]^{\dagger}\right)/2, & \tilde{X}_{+-} &:= \hat{P}\left([0,0,1,1]^{\dagger}\right)/2,\\
\tilde{X}_{-+} &:= \hat{P}\left([0,0,-1,1]^{\dagger}\right)/2, & \tilde{X}_{--} &:= \hat{P}\left([1,-1,0,0]^{\dagger}\right)/2,\\
\tilde{Y}_{++} &:= \hat{P}([1,0,1,0])/2, & \tilde{Y}_{+-} &:= \hat{P}([0,1,0,1])/2,\\
\tilde{Y}_{-+} &:= \hat{P}([0,-1,0,1])/2, & \tilde{Y}_{--} &:= \hat{P}([1,0,-1,0])/2.
\end{aligned} \tag{C6}$$

We notice that

$$\begin{aligned}
E_{\mathbb{1},\mathbb{1}}^{(l,i,k,k')} + E_{X,\mathbb{1}}^{(l,i,k,k')} &= a'^{*}_{0}a_0 + a'^{*}_{1}a_1 + a'^{*}_{1}a_0 + a'^{*}_{0}a_1 + a'^{*}_{2}a_2 + a'^{*}_{3}a_3 - a'^{*}_{3}a_2 - a'^{*}_{2}a_3\\
&= \left(a_0'^{*} + a_1'^{*}\right)(a_0 + a_1) + \left(-a_2'^{*} + a_3'^{*}\right)(-a_2 + a_3)\\
&= {B_{k'}^{(l,i)}}^{\dagger}\left[\tilde{X}_{++} + \tilde{X}_{-+}\right]B_k^{(l,i)}\\
&= {B_{k'}^{(l,i)}}^{\dagger}\hat{T}_{0_X,\hat{\mathbb{1}}}B_k^{(l,i)},
\end{aligned} \tag{C7}$$

where we defined

$$B_k^{(l,i)} := \begin{pmatrix} a_0^{(l,i,k)} & a_1^{(l,i,k)} & a_2^{(l,i,k)} & a_3^{(l,i,k)} \end{pmatrix}^{T}, \tag{C8}$$

and

$$\hat{T}_{0_X,\mathbb{1}} := \tilde{X}_{++} + \tilde{X}_{-+}. \tag{C9}$$

We can proceed similarly for all terms in the form of equation (C4) to find

$$E_{\mathbb{1},\omega}^{(l,i,k,k')} + (-1)^{s}E_{X,\omega}^{(l,i,k,k')} = {B_{k'}^{(l,i)}}^{\dagger}\hat{T}_{s_X,\omega}B_k^{(l,i)}, \tag{C10}$$

with

$$\begin{aligned}
\hat{T}_{1_X,\mathbb{1}} &= \tilde{X}_{--} + \tilde{X}_{+-},\\
\hat{T}_{0_X,X} &= \tilde{X}_{++} - \tilde{X}_{-+},\\
\hat{T}_{1_X,X} &= -\tilde{X}_{--} + \tilde{X}_{+-},\\
\hat{T}_{0_X,Z} &= \tilde{Z}_{00} + \tilde{Z}_{01} - \tilde{Y}_{-+} - \tilde{Y}_{++},\\
\hat{T}_{1_X,Z} &= -\tilde{Z}_{11} - \tilde{Z}_{10} + \tilde{Y}_{-+} + \tilde{Y}_{++}.
\end{aligned}$$

Let now

$$\hat{B}^{(l,i)} = \begin{pmatrix} a_0^{(l,i,0)} & a_0^{(l,i,1)} & \dots \\ a_1^{(l,i,0)} & a_1^{(l,i,1)} & \dots \\ a_2^{(l,i,0)} & a_2^{(l,i,1)} & \dots \\ a_3^{(l,i,0)} & a_3^{(l,i,1)} & \dots \end{pmatrix} = \begin{pmatrix} B_0^{(l,i)} & B_1^{(l,i)} & \dots \end{pmatrix}, \tag{C11}$$

and

$$\left|\Gamma^{(l,i)}\right\rangle = \begin{pmatrix} \left|\gamma^{(l,i,0)}\right\rangle \\ \left|\gamma^{(l,i,1)}\right\rangle \\ \vdots \end{pmatrix}. \tag{C12}$$

One can easily check that

$${B_{k'}^{(l,i)}}^{\dagger}\hat{T}_{s_X,\omega}B_k^{(l,i)} = \left(\hat{B}^{(l,i)\dagger}\hat{T}_{s_X,\omega}\hat{B}^{(l,i)}\right)_{k'k}, \tag{C13}$$

and consequently, from equation (B25) we have that

$$\begin{aligned} q^{virt,(l)}_{s_X,\omega} &= \frac{1}{2}\sum_{i,k,k'} \left\langle \gamma^{(l,i,k')} \middle| \hat{C}^\dagger \hat{C} \middle| \gamma^{(l,i,k)} \right\rangle_T \mathrm{Tr}\left[\hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})\dagger}_{i,k';B|O_{l-1}} |s_X\rangle\langle s_X|_B \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,k;B|O_{l-1}} \hat{\sigma}_\omega \right] \\ &= \frac{1}{2}\sum_{i,k,k'} \left\langle \gamma^{(l,i,k')} \middle| \hat{C}^\dagger \hat{C} \middle| \gamma^{(l,i,k)} \right\rangle_T \left(\hat{B}^{(l,i)\dagger} \hat{T}_{s_X,\omega} \hat{B}^{(l,i)} \right)_{k'k} \\ &= \frac{1}{2}\sum_{i} \left\langle \Gamma^{(l,i)} \middle| \left[\hat{B}^{(l,i)\dagger} \hat{T}_{s_X,\omega} \hat{B}^{(l,i)} \otimes \hat{C}^\dagger \hat{C} \right] \middle| \Gamma^{(l,i)} \right\rangle \\ &= \frac{1}{2}\sum_{i} \left\langle \Phi^{(l,i)} \middle| \hat{T}_{s_X,\omega} \otimes \hat{C}^\dagger \hat{C} \middle| \Phi^{(l,i)} \right\rangle, \end{aligned} \tag{C14}$$

where we have defined (recall equation (B8))

$$\left|\Phi^{(l,i)}\right\rangle := \left(\hat{B}^{(l,i)} \otimes \hat{\mathbb{1}}_T\right) \left|\Gamma^{(l,i)}\right\rangle = \begin{pmatrix} a_0^{(l,i,0)} \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,0;B|O_{l-1}} & a_0^{(l,i,1)} \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,1;B|O_{l-1}} & \cdots \\ a_1^{(l,i,0)} \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,0;B|O_{l-1}} & a_1^{(l,i,1)} \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,1;B|O_{l-1}} & \cdots \\ a_2^{(l,i,0)} \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,0;B|O_{l-1}} & a_2^{(l,i,1)} \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,1;B|O_{l-1}} & \cdots \\ a_3^{(l,i,0)} \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,0;B|O_{l-1}} & a_3^{(l,i,1)} \hat{A}^{(\vec{x}_{<l},\vec{x}_{>l})}_{i,1;B|O_{l-1}} & \cdots \end{pmatrix} \begin{pmatrix} |0\rangle_T \\ \vdots \\ |0\rangle_T \end{pmatrix}. \tag{C15}$$

By taking the sum over l of equation (C14) and letting

$$\hat{\rho}_E := \sum_{l,i} \left|\Phi^{(l,i)}\right\rangle\left\langle\Phi^{(l,i)}\right|, \tag{C16}$$

one obtains the result in equation (B26). Finally, by comparing equations (B11)–(B15) and equations (B24) and (B25), we observe that a formulation equivalent to the one leading to equation (C14) can be done for the terms $q_{s_X,\omega|O^{(l-1)}}$ in equation (B15) with the substitution $\hat{C}^\dagger \hat{C} \mapsto \hat{F}_s{}^\dagger \hat{F}_s$, for $s \in \{0,1\}$, which yields the result in equation (B27).

ORCID iDs

Alessandro Marcomini https://orcid.org/0009-0000-3577-029X
Akihiro Mizutani https://orcid.org/0009-0008-5161-253X
Fadri Grünenfelder https://orcid.org/0000-0003-3421-0922
Marcos Curty https://orcid.org/0000-0002-0330-6828
Kiyoshi Tamaki https://orcid.org/0000-0002-6446-5769

References

[1] Lo H-K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595
[2] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 *Rev. Mod. Phys.* **92** 025002
[3] Pirandola S *et al* 2020 *Adv. Opt. Photonics* **12** 1012
[4] Dynes J F *et al* 2019 *npj Quantum Inf.* **5** 1
[5] Stucki D *et al* 2011 *New J. Phys.* **13** 123001
[6] Sasaki M *et al* 2011 *Opt. Express* **19** 10387
[7] Chen Y-A *et al* 2021 *Nature* **589** 214
[8] Liao S-K *et al* 2017 *Nature* **549** 43
[9] ThinkQuantum 2024 (available at: www.thinkquantum.com/) (Accessed 26 September 2024)
[10] ID Quantique 2024 (available at: www.idquantique.com) (Accessed 26 September 2024)
[11] Toshiba 2024 (available at: www.toshiba.eu/quantum/) (Accessed 26 September 2024)
[12] Bundesamt für Sicherheit in der Informationstechnik 2024 A study on implementation attacks against QKD systems (available at: www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html) (Accessed 15 November 2024)
[13] Jain N, Stiller B, Khan I, Elser D, Marquardt C and Leuchs G 2016 *Contemp. Phys.* **57** 366
[14] Sun S and Huang A 2022 *Entropy* **24** 260
[15] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 *Phys. Rev.* A **78** 042333
[16] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[17] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 *Nat. Commun.* **2** 349
[18] Weier H, Krauss H, Rau M, Fürst M, Nauerth S and Weinfurter H 2011 *New J. Phys.* **13** 073024
[19] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev. Lett.* **107** 110501
[20] Lu F-Y *et al* 2023 *Optica* **10** 520
[21] Pang X-L, Yang A-L, Zhang C-N, Dou J-P, Li H, Gao J and Jin X-M 2020 *Phys. Rev. Appl.* **13** 034008
[22] Tan H, Zhang W-Y, Zhang L, Li W, Liao S-K and Xu F 2022 *Quantum Sci. Technol.* **7** 045008

[23] Ye P et al 2023 Phys. Rev. Appl. 19 054052
[24] Wu Z, Huang A, Chen H, Sun S-H, Ding J, Qiang X, Fu X, Xu P and Wu J 2020 Opt. Express 28 25574
[25] Zhang X-X, Jiang M-S, Wang Y, Lu Y-F, Li H-W, Zhou C, Zhou Y and Bao W-S 2022 Phys. Rev. A 106 062412
[26] Baliuka A, Stöcker M, Auer M, Freiwang P, Weinfurter H and Knips L 2023 Phys. Rev. Appl. 20 054040
[27] Zapatero V, Navarrete A and Curty M 2024 Adv. Quantum Technol. 7 2300380
[28] Sajeed S, Minshull C, Jain N and Makarov V 2017 Sci. Rep. 7 8403
[29] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C and Leuchs G 2014 New J. Phys. 16 123030
[30] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt C, Makarov V and Leuchs G 2011 New J. Phys. 13 013043
[31] Yuan Z L, Dynes J F and Shields A J 2011 Appl. Phys. Lett. 98 231104
[32] Yuan Z L, Dynes J F and Shields A J 2011 Appl. Phys. Lett. 99 196102
[33] Sajeed S, Chaiwongkhot P, Bourgoin J-P, Jennewein T, Lütkenhaus N and Makarov V 2015 Phys. Rev. A 91 062301
[34] Rau M, Vogl T, Corrielli G, Vest G, Fuchs L, Nauerth S and Weinfurter H 2015 IEEE J. Sel. Top. Quantum Electron. 21 187
[35] Chaiwongkhot P, Kuntz K B, Zhang Y, Huang A, Bourgoin J-P, Sajeed S, Lütkenhaus N, Jennewein T and Makarov V 2019 Phys. Rev. A 99 062315
[36] Wei K, Zhang W, Tang Y-L, You L and Xu F 2019 Phys. Rev. A 100 022325
[37] Fung C-H F, Tamaki K, Qi B, Lo H-K and Ma X 2009 Quantum Inf. Comput. 9 131–65
[38] Lydersen L and Skaar J 2008 Quantum Inf. Comput. 10 60
[39] Ma J, Zhou Y, Yuan X and Ma X 2019 Phys. Rev. A 99 062325
[40] Bochkov M K and Trushechkin A S 2019 Phys. Rev. A 99 032308
[41] Zhang Y, Coles P J, Winick A, Lin J and Lütkenhaus N 2021 Phys. Rev. Res. 3 013076
[42] Trushechkin A 2022 Quantum 6 771
[43] Tupkary D, Nahar S, Sinha P and Lütkenhaus N 2024 Phase error rate estimation in QKD with imperfect detectors (arXiv:2408.17349 [quant-ph])
[44] Hwang W-Y 2003 Phys. Rev. Lett. 91 057901
[45] Wang X-B 2005 Phys. Rev. Lett. 94 230503
[46] Lo H-K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
[47] Ma X, Qi B, Zhao Y and Lo H-K 2005 Phys. Rev. A 72 012326
[48] Lim C C W, Curty M, Walenta N, Xu F and Zbinden H 2014 Phys. Rev. A 89 022307
[49] Tamaki K, Curty M, Kato G, Lo H-K and Azuma K 2014 Phys. Rev. A 90 052314
[50] Pereira M, Curty M and Tamaki K 2019 npj Quantum Inf. 5 62
[51] Pereira M, Kato G, Mizutani A, Curty M and Tamaki K 2020 Sci. Adv. 6 eaaz4487
[52] Zapatero V, Navarrete A, Tamaki K and Curty M 2021 Quantum 5 602
[53] Currás-Lorenzo G, Nahar S, Lütkenhaus N, Tamaki K and Curty M 2024 Quantum Sci. Technol. 9 015025
[54] Currás-Lorenzo G, Pereira M, Kato G, Curty M and Tamaki K 2023 A security framework for quantum key distribution implementations (arXiv:2305.05930 [quant-ph])
[55] Lu F-Y et al 2022 Optica 9 886
[56] Lu F-Y et al 2023 Phys. Rev. Lett. 131 110802
[57] Lo H-K, Curty M and Qi B 2012 Phys. Rev. Lett. 108 130503
[58] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Nature 557 400
[59] Wang S et al 2022 Nat. Photon. 16 154
[60] Liu Y et al 2023 Phys. Rev. Lett. 130 210801
[61] Liu J-Y, Ma X, Ding H-J, Zhang C-H, Zhou X-Y and Wang Q 2023 Phys. Rev. A 108 022605
[62] Koashi M 2009 New J. Phys. 11 045018
[63] Lo H-K and Preskill J 2007 Quantum Inf. Comput. 7 431
[64] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Phys. Rev. A 54 3824
[65] Bennett C H, Bernstein H J, Popescu S and Schumacher B 1996 Phys. Rev. A 53 2046
[66] ID qube NIR free-running 2024 (available at: www.idquantique.com/quantum-detection-systems/products/id-qube-nir-free-running/) (Accessed 15 November 2024)
[67] Fei Y et al 2022 Opt. Express 30 36456
[68] Knoll G F 2000 Radiation Detection and Measurement 3rd edn (Wiley)
[69] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 Quantum Inf. Comput. 4 325
[70] Kato G 2020 Concentration inequality using unconfirmed knowledge (arXiv:2002.04357 [math.PR])
[71] Azuma K 1967 Tohoku Math. J. 19 357