IOP Publishing Quantum Sci. Technol. 8 (2023) 025014 https://doi.org/10.1088/2058-9565/acbc46

Quantum Science and Technology

OPEN ACCESS

RECEIVED
25 October 2022

REVISED
11 January 2023

ACCEPTED FOR PUBLICATION
15 February 2023

PUBLISHED
27 February 2023

PAPER

A fully passive transmitter for decoy-state quantum key distribution

Víctor Zapatero[1,2,3,*], **Wenyuan Wang**[4] and **Marcos Curty**[1,2,3]

[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] Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong, People's Republic of China
[*] Author to whom any correspondence should be addressed.

E-mail: vzapatero@com.uvigo.es

Keywords: quantum cryptography, quantum key distribution, passive encoding

Abstract

A passive quantum key distribution (QKD) transmitter generates the quantum states prescribed by a QKD protocol at random, combining a fixed quantum mechanism and a post-selection step. By circumventing the use of active optical modulators externally driven by random number generators, passive QKD transmitters offer immunity to modulator side channels and potentially enable higher frequencies of operation. Recently, the first linear optics setup suitable for passive decoy-state QKD has been proposed. In this work, we simplify the prototype and adopt sharply different approaches for BB84 polarization encoding and decoy-state parameter estimation. In particular, our scheme avoids a probabilistic post-selection step that is central to the former proposal. On top of it, we elaborate a simple and tight custom-made security analysis.

1. Introduction

Quantum key distribution (QKD) allows for information-theoretically secure key exchange between distant parties through an insecure channel [1, 2]. This possibility, which is inaccessible from the point of view of classical communications, makes QKD a promising candidate for long-term communication security. Nowadays, QKD represents one of the most mature applications of quantum information science, and it is expected to become a prolific industry in the years to come. Notwithstanding, the security of real QKD implementations is not fully established yet, due to the difficulty of experimentally guaranteeing that the QKD devices stick to the assumptions and models presumed in the security proofs [3].

A particularly controversial assumption of most QKD security analyses is that no information leakage occurs through the boundaries of Alice's and Bob's labs. This premise opens the door for the so-called Trojan horse attacks (THAs) [4–8], where an adversary injects bright light pulses into a QKD transmitter/receiver and then measures the back-reflected light, aiming to extract information about the setting choices. Notably, a possible solution to deal with information leakage in the QKD transmitter consists of trying to upper bound Eve's accessible information gain and account for it in the estimation of the secret key length [9–12]. Note, however, that this approach relies on modelling the information leakage to a certain extent, and it requires to add significant optical isolation to prevent a severe drop of the secret key rate and the achievable distance.

On the contrary, an alternative solution that might rule out THAs once and for all is to consider a fully passive (rather than active) QKD transmitter, as illustrated in figure 1.

In a passive transmitter (PT), the protocol states are generated at random using inherent quantum randomness of the device, in so avoiding the use of quantum random number generators (QRNGs) to actively modulate the protocol settings (e.g. intensity, phase or polarization), or the use of auxiliary optical modulators of any kind. Indeed, the advantages of passive encoding go beyond the obvious security upgrade. To be precise, the fact that a PT avoids using externally driven elements makes it very desirable to operate QKD systems at high transmission rates, and to reduce the complexity (and thus the cost) of practical QKD

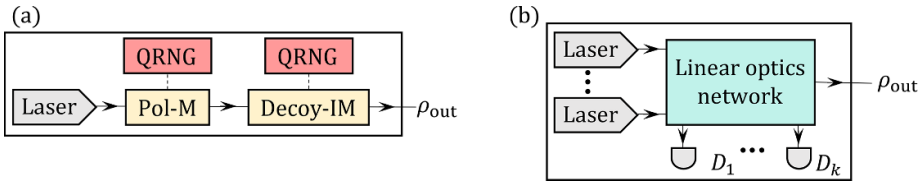

Figure 1. Schematic depiction of (a) active and (b) passive decoy-state QKD transmission. In the active case, a polarization modulator (Pol-M) and an intensity modulator (Decoy-IM) are driven by respective quantum random number generators (QRNGs), responsible for implementing the protocol settings. In the passive case, one or more laser diodes generate pulses that are sent through a linear optics network. Depending on the detection outcomes observed in the photodetectors ($\{D_j\}$), different signal states are actually generated, avoiding the use of active modulators or QRNGs.

implementations [13]. Indeed, the possibility to reach an enhanced bandwidth by suppressing active modulation has already been realized in [14], where the construction a modulator-free (although active) QKD transmission chip is reported.

However, these advantages come at the price of decreasing the key generation rate for two main reasons. On the one hand, in a PT, additional sifting is required to discard those rounds where the randomly generated settings do not lie in certain acceptance regions. On the other hand, the finite size of these acceptance regions is an inherent source of noise not present in the active case.

Various proposals exist for passive decoy-state generation with parametric down-conversion sources [15–20], or using coherent light [21–24]. Notably, both alternatives have been demonstrated experimentally [25–30]. In parallel, a simple alternative to passively generate random photon polarizations in a plane was reported in [31], suitable for a passive implementation of the BB84 protocol [32]. What is more, a PT preparing decoy-state BB84 signals with coherent pulses was introduced in [33]. Nevertheless, this latter proposal relies on a non-linear optical effect called sum-frequency generation [34], which reduces its practicality.

In short, a simple setup simultaneously generating random decoy states and random photon polarizations in a fully passive way remained elusive for more than a decade. Recently though, a linear-optics-based PT of this kind has been proposed in [35], combining the ideas of [22] and [31]. Specifically, in [35], a passive decoy-state BB84 protocol is considered, using a single intensity for the key generation basis and three different intensities for the parameter estimation basis. In the present work, we devise a simplified architecture for the prototype presented there and consider the standard decoy-state BB84 protocol instead, with three common intensity settings per basis. For symmetry reasons, our protocol uses both bases for key generation.

Remarkably as well, to avoid the assessment of the security analysis with mixed polarization states, the proposal in [35] relies on a facilitating assumption. Namely, that the actual protocol can be reduced to an ideal one where perfect Bell pairs are prepared for the single photon events and the effect of the mixed polarizations is incorporated *a posteriori*, adding post-processing noise at Alice's local measurements. Here, we circumvent this assumption by elaborating a custom-made security analysis for the mixed single-photon states.

On top of it, the decoy-state method in [35] relies on an auxiliary post-selection probability to decouple the intensity and the polarization of the output Fock states of the PT in the parameter estimation basis. This step, which entails an undesired discard of raw data, requires a QRNG and might be cumbersome to implement in practice. In this work, we avoid this extra sifting by tackling the decoy-state parameter estimation with the intensity-setting-dependent Fock states directly.

The structure of the paper goes as follows. We present the PT and its mixed output state in section 2. In section 3 we describe a simple approach to post-select decoy-state BB84 acceptance regions, together with the quantum states that arise from this post-selection. Section 4 is dedicated to explain our decoy-state parameter estimation method, and in section 5 we derive the single-photon phase-error rate of the problem at hand. Coming next, in section 6 we evaluate the rate-distance performance of our passive QKD scheme and compare it to the performance achieved in the active setting. Finally, section 7 provides a summarizing discussion, and a series of appendices are included at the end of the paper to ensure the reproducibility of the results.

2. A passive QKD transmitter

The PT we propose is depicted in figure 2. In the figure, we use the notation $|\tau\rangle_{a,\mathrm{R(L)}}$ to denote a right-handed (left-handed) circularly polarized weak coherent pulse (WCP) in the spatial mode a with

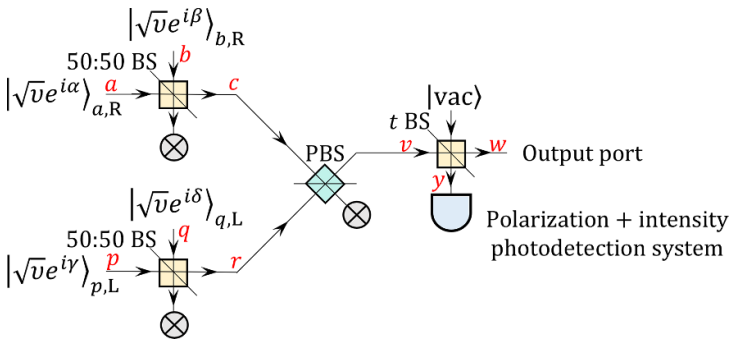

Figure 2. Architecture of the PT. All input coherent states in the figure have a common large intensity ν and independent random phases α, β, γ and δ. Red color is used to denote the relevant spatial modes, while unused modes are tagged by the symbol '$\otimes$'. The interference occurring in the 50:50 beamsplitter (BS) of the top (bottom) arm yields a coherent state with a random intensity dependent on the phase difference $\beta-\alpha$ ($\delta-\gamma$), while the polarization —common to both input states— is preserved. Crucially, the polarization of the top arm (right-handed) is orthogonal to that of the bottom arm (left-handed). When combined in the polarizing BS (PBS), these orthogonally polarized coherent pulses generate a final coherent state with random intensity and random polarization in the RL Bloch sphere, coupled to each other. Lastly, this state enters a BS with transmittance $t \ll 1$, where the intensity is attenuated to the single-photon level. Importantly, while the transmitted signal goes to the quantum channel, the reflected signal reaches a photo-detection system that accurately measures its polarization and intensity for post-selection purposes.

complex amplitude $\tau \in \mathbb{C}$. Namely, $|\tau\rangle_{a,\mathrm{R(L)}} = \exp\{\tau a^\dagger_{\mathrm{R(L)}} - \tau^* a_{\mathrm{R(L)}}\}\,|\mathrm{vac}\rangle$, where $|\mathrm{vac}\rangle$ is the vacuum state and $\{a^\dagger_{\mathrm{R(L)}}, a_{\mathrm{R(L)}}\}$ denote the creation/annihilation operators of a right-handed (left-handed) circular polarization state in spatial mode a. Notably, $a^\dagger_{\mathrm{R}}|\mathrm{vac}\rangle$ and $a^\dagger_{\mathrm{L}}|\mathrm{vac}\rangle$ shall be viewed as the north and the south pole of a Bloch sphere throughout this work, which we shall refer to as 'the RL Bloch sphere'. The selection of the circularly polarized single-photon states as the poles of the sphere is such that the equator plane of the sphere contains all possible linearly polarized single-photon states, the specific orientation being determined by the azimuthal angle. In particular, the creation operator associated to an arbitrary polarization (θ,ϕ) in the RL Bloch sphere reads

$$a^\dagger_{\theta,\phi} = \cos\left(\frac{\theta}{2}\right) a^\dagger_{\mathrm{R}} + e^{i\phi}\sin\left(\frac{\theta}{2}\right) a^\dagger_{\mathrm{L}}, \tag{1}$$

where θ (ϕ) stands for the polar (azimuthal) angle of the sphere. Also, a WCP in spatial mode a, with amplitude τ and polarization specified by (θ,ϕ) shall be denoted as $|\tau\rangle_{a,\theta,\phi}$. This said, let us present the output state of the PT.

Instead of referring to the independent and identically distributed phases α, β, γ and δ of figure 2, the output state of the PT is better described in terms of the parameters α, $\delta_1 = \beta-\alpha$, $\delta_2 = \gamma-\beta$ and $\delta_3 = \delta-\gamma$, the last three phase differences being uniformly random and independent too. Particularly, for specific values of α, δ_1, δ_2 and δ_3, the output state at mode w in figure 2 reads

$$|\Psi\rangle_w = \left|\sqrt{I(\delta_1,\delta_3)}\; e^{i\psi(\alpha,\delta_1)}\right\rangle_{w,\theta(\delta_1,\delta_3),\phi(\delta_1,\delta_2,\delta_3)}, \tag{2}$$

where the quantities $I(\delta_1,\delta_3)$, $\psi(\alpha,\delta_1)$, $\theta(\delta_1,\delta_3)$ and $\phi(\delta_1,\delta_2,\delta_3)$ are given by

$$\begin{aligned}
I(\delta_1,\delta_3) &= 2\nu t\left[\sin^2\left(\frac{\delta_1}{2}\right)+\sin^2\left(\frac{\delta_3}{2}\right)\right]\ \text{(intensity)},\\
\psi(\alpha,\delta_1) &= \alpha+\frac{\delta_1-\pi}{2}\ \text{(phase)},\\
\theta(\delta_1,\delta_3) &= 2\arctan\left[\sin\left(\frac{\delta_3}{2}\right)\Big/\sin\left(\frac{\delta_1}{2}\right)\right]\ \text{(polar angle in the RL Bloch sphere)},\\
\phi(\delta_1,\delta_2,\delta_3) &= \delta_2+\frac{\delta_1+\delta_3}{2}\ \text{(azimuthal angle in the RL Bloch sphere)}.
\end{aligned} \tag{3}$$

This is proven in appendix A using standard linear quantum optics.

If we now assume perfect phase-randomisation for the input coherent states, the mixed output state of the transmitter is

$$\sigma_w = \frac{1}{(2\pi)^4}\int_0^{2\pi}\int_0^{2\pi}\int_0^{2\pi}\int_0^{2\pi} \mathrm{d}\alpha\mathrm{d}\delta_1\mathrm{d}\delta_2\mathrm{d}\delta_3 |\Psi\rangle\langle\Psi|_w. \tag{4}$$

The integral in α is direct (the purpose of changing variables from β, γ and δ to δ_1, δ_2 and δ_3 is to enable this immediate integration in α) and yields a phase-randomised WCP,

$$\frac{1}{2\pi}\int_0^{2\pi} \mathrm{d}\alpha |\Psi\rangle\langle\Psi|_w = \sum_{n=0}^{\infty} \frac{e^{-I}I^n}{n!} |n\rangle\langle n|_{\theta,\phi}, \tag{5}$$

with the n-photon Fock states $|n\rangle_{\theta,\phi}$ given by

$$|n\rangle_{\theta,\phi} = \frac{\left(w^{\dagger}_{\theta,\phi}\right)^n}{\sqrt{n!}} |\mathrm{vac}\rangle\,. \tag{6}$$

Note that we have omitted the dependence on δ_1, δ_2 and δ_3 in equation (5) for readability. Also, the spatial mode w is not explicitly indicated any more.

The phase differences δ_1, δ_2 and δ_3 uniquely determine the relevant output variables ϕ, θ and I, and it is desirable to describe the output state of the transmitter (given in equation (4)) in terms of the latter instead. The joint probability density function $f_{\boldsymbol{\phi},\boldsymbol{\theta},\boldsymbol{I}}(\phi,\theta,I)$ is obtained in appendix B and factors as

$$f_{\boldsymbol{\phi},\boldsymbol{\theta},\boldsymbol{I}}(\phi,\theta,I) = f_{\boldsymbol{\phi}}(\phi) \times f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I), \tag{7}$$

where

$$f_{\boldsymbol{\phi}}(\phi) = \frac{1}{2\pi} \text{ and } f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I) = \frac{1}{2\nu t\pi^2\sqrt{1-\frac{I}{2\nu t}\cos^2\left(\frac{\theta}{2}\right)}\sqrt{1-\frac{I}{2\nu t}\sin^2\left(\frac{\theta}{2}\right)}}, \tag{8}$$

for $\phi \in (-\pi,\pi]$, $\theta \in [0,\pi]$ and $I \in [0, I_{\max,\theta})$, $I_{\max,\theta}$ being defined as $I_{\max,\theta} = \min\left\{2\nu t/\cos^2(\theta/2)\,,\right.$ $\left.2\nu t/\sin^2(\theta/2)\right\}$.

Notably, the above distribution exhibits azimuthal symmetry and is peaked towards the equator plane of the RL Bloch sphere, given by $\theta = \pi/2$. This makes the proposed architecture convenient for a passive decoy-state BB84 protocol using 'equator-plane BB84 states'. In the next section, we elaborate on this idea.

3. Post-selection of BB84 acceptance regions

From equation (4) to equation (8), it follows that the mixed output state of the transmitter reads

$$\sigma = \frac{1}{2\pi}\int_{-\pi}^{\pi}\mathrm{d}\phi\int_0^{\pi}\mathrm{d}\theta\int_0^{I_{\max,\theta}}\mathrm{d}I f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I)\sum_{n=0}^{\infty}\frac{e^{-I}I^n}{n!}|n\rangle\langle n|_{\theta,\phi} \tag{9}$$

if no post-selection step is performed. Coming next, we define acceptance regions in the (ϕ,θ,I) space for the post-selection, which are presumed to be accurately identified by the photo-detection system in figure 2. For the standard decoy-state BB84 protocol with three intensity settings, an obvious choice is

$$\Omega_{x,j} = \left\{\phi \in (x-\Delta\phi, x+\Delta\phi)\,, \theta \in \left(\frac{\pi}{2}-\Delta\theta, \frac{\pi}{2}+\Delta\theta\right), I \in I_j\right\}, \tag{10}$$

where $x \in \{0,\pi,\pi/2,-\pi/2\}$ tags the BB84 polarization states, $\Delta\phi \in (0,\pi/4)$ and $\Delta\theta \in (0,\pi/2)$ define the angular widths of the acceptance regions in the RL Bloch sphere (see figure 3), and I_j stands for the interval of intensities that defines the jth intensity setting, $j \in \{\mathrm{s}$ ('signal'), d ('decoy'), v ('vacuum')$\}$. As the notation suggests, we shall assume below that the key is extracted from the signal setting, while the decoy and the vacuum settings are only used for parameter estimation.

The resulting post-selected states read $\sigma_{x,j} = \tilde{\sigma}_{x,j}/\mathrm{Tr}\left[\tilde{\sigma}_{x,j}\right]$ for

$$\tilde{\sigma}_{x,j} = \frac{1}{2\pi}\int_{x-\Delta\phi}^{x+\Delta\phi}\mathrm{d}\phi\int_{\frac{\pi}{2}-\Delta\theta}^{\frac{\pi}{2}+\Delta\theta}\mathrm{d}\theta\int_{I_j}\mathrm{d}I f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I)\sum_{n=0}^{\infty}\frac{e^{-I}I^n}{n!}|n\rangle\langle n|_{\theta,\phi}. \tag{11}$$

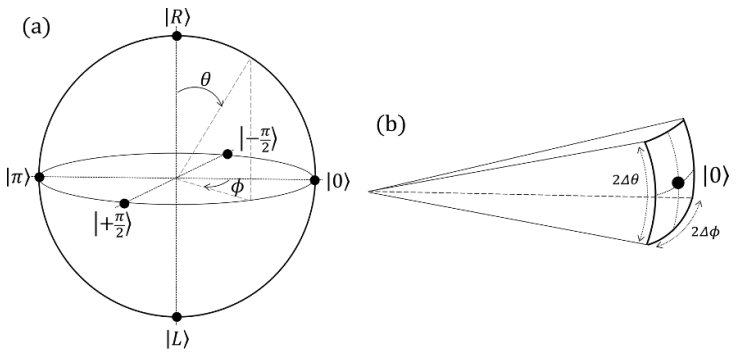

Figure 3. Post-selection of BB84 acceptance regions in the RL Bloch sphere. The sphere is illustrated in figure (a). θ (ϕ) provides the polar (azimuthal) angle, $|R\rangle = a_{\mathrm{R}}^{\dagger}|\mathrm{vac}\rangle$ ($|L\rangle = a_{\mathrm{L}}^{\dagger}|\mathrm{vac}\rangle$) denotes a right-handed (left-handed) circularly polarized single-photon state, and $\left\{|x\rangle = \left(|\mathrm{R}\rangle + e^{ix}|\mathrm{L}\rangle\right)/\sqrt{2}\right\}$ with $x \in \{0, \pi, \pi/2, -\pi/2\}$ defines a set of four linearly polarized single-photon states evenly spaced in the equator line, suitable for an ideal implementation of the BB84. Figure (b) exemplifies the acceptance polarization region associated to the BB84 state $|0\rangle$, given by a rectangular solid angle centered in this state with angular widths $2\Delta\phi$ and $2\Delta\theta$.

Note that

$$\mathrm{Tr}\left[\tilde{\sigma}_{x,j}\right] = \frac{1}{2\pi}\int_{x-\Delta\phi}^{x+\Delta\phi}\mathrm{d}\phi\int_{\frac{\pi}{2}-\Delta\theta}^{\frac{\pi}{2}+\Delta\theta}\mathrm{d}\theta\int_{I_j}\mathrm{d}I f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I) = \frac{\Delta\phi}{\pi}\int_{\frac{\pi}{2}-\Delta\theta}^{\frac{\pi}{2}+\Delta\theta}\mathrm{d}\theta\int_{I_j}\mathrm{d}I f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I). \tag{12}$$

That is to say, $\mathrm{Tr}\left[\tilde{\sigma}_{x,j}\right]$ provides the probability that the output state lies in the acceptance region $\Omega_{x,j}$. Notably as well, given the set $\{\Omega_{x,j}\}_x$, the Z (X) basis acceptance region associated to the jth intensity setting is constructed as $\Omega_j^Z = \Omega_{0,j}\cup\Omega_{\pi,j}$ ($\Omega_j^X = \Omega_{\frac{\pi}{2},j}\cup\Omega_{-\frac{\pi}{2},j}$).

In what follows, we shall use the shorthand notation $\langle\cdot\rangle_{\Omega}$ to denote the triple integral of any input '$\cdot$' weighted by $f_{\boldsymbol{\phi},\boldsymbol{\theta},\boldsymbol{I}}(\phi,\theta,I) = f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I)/2\pi$ in the region Ω of the (ϕ,θ,I)-space. As an example, with this convention equation (11) reads

$$\tilde{\sigma}_{x,j} = \left\langle\sum_{n=0}^{\infty}\frac{e^{-I}I^n}{n!}|n\rangle\langle n|_{\theta,\phi}\right\rangle_{\Omega_{x,j}}, \tag{13}$$

and $\mathrm{Tr}\left[\tilde{\sigma}_{x,j}\right] = \langle 1\rangle_{\Omega_{x,j}}$. Also, with this notation, it is obvious that $\sigma_{x,j}$ is a convex combination of Fock states. To be precise, normalizing equation (13) immediately yields

$$\sigma_{x,j} = \sum_{n=0}^{\infty} p\left(n|\Omega_{x,j}\right)\sigma_{x,j,n}, \tag{14}$$

where $p\left(n|\Omega_{x,j}\right) = \left\langle\frac{e^{-I}I^n}{n!}\right\rangle_{\Omega_{x,j}}\Big/\langle 1\rangle_{\Omega_{x,j}}$ and

$$\sigma_{x,j,n} = \frac{\left\langle\frac{e^{-I}I^n}{n!}|n\rangle\langle n|_{\theta,\phi}\right\rangle_{\Omega_{x,j}}}{\left\langle\frac{e^{-I}I^n}{n!}\right\rangle_{\Omega_{x,j}}} \tag{15}$$

is a Fock state with photon number n. Notably, the conditional photon-number statistics $p\left(n|\Omega_{x,j}\right)$ are independent of x because of the azimuthal symmetry. Therefore, below we shall denote $p\left(n|\Omega_{x,j}\right)$ simply as $p_{n|j}$ for all x.

Similarly, the same symmetry shows that, if we focus on the acceptance region $\Omega_j^Z = \Omega_{0,j}\cup\Omega_{\pi,j}$, the post-selected output state of the transmitter reads

$$\sigma_j^Z = \frac{1}{\langle 1\rangle_{\Omega_j^Z}}\left\langle\sum_{n=0}^{\infty}\frac{e^{-I}I^n}{n!}|n\rangle\langle n|_{\theta,\phi}\right\rangle_{\Omega_j^Z} = \sum_{n=0}^{\infty}p_{n|j}\sigma_{j,n}^Z \tag{16}$$

with $\sigma_{j,n}^Z = \left(\sigma_{0,j,n} + \sigma_{\pi,j,n}\right)/2$.

Identically, for the X basis we have $\sigma_j^X = \sum_{n=0}^{\infty}p_{n|j}\sigma_{j,n}^X$ with $\sigma_{j,n}^X = \left(\sigma_{\frac{\pi}{2},j,n} + \sigma_{-\frac{\pi}{2},j,n}\right)/2$.

4. Decoy-state analysis

In this section, we present the decoy-state equations for the Z basis, and the ones for the X basis are discussed at the end.

In the first place, it is necessary to introduce some notation. Let Q_j^Z (E_j^Z) be the probability that a 'click' (an 'error') is recorded conditioned on the event that σ_j^Z is post-selected and Bob performs his measurement in the Z basis. Namely, $Q_j^Z = p\left(\text{click}|\sigma_j^Z, Z\right)$ and $E_j^Z = p\left(\text{err}|\sigma_j^Z, Z\right)$. Similarly, let $y_{j,n}^Z$ and $e_{j,n}^Z$ denote the corresponding n-photon yield and n-photon error probability, respectively, such that $y_{j,n}^Z = p\left(\text{click}|\sigma_{j,n}^Z, Z\right)$ and $e_{j,n}^Z = p\left(\text{err}|\sigma_{j,n}^Z, Z\right)$.

From the above definitions and equation (16), it follows that $Q_j^Z = \sum_{n=0}^{\infty} p_{n|j} y_{j,n}^Z$ and $E_j^Z = \sum_{n=0}^{\infty} p_{n|j} e_{j,n}^Z$ for all j. Therefore, truncating the sums to a threshold photon number n_{cut}, we find the constraints

$$\begin{cases} Q_j^Z \geqslant \sum_{n=0}^{n_{\text{cut}}} p_{n|j} y_{j,n}^Z, \\ Q_j^Z \leqslant \sum_{n=0}^{n_{\text{cut}}} p_{n|j} y_{j,n}^Z + 1 - \sum_{n=0}^{n_{\text{cut}}} p_{n|j} \end{cases} \quad \text{and} \quad \begin{cases} E_j^Z \geqslant \sum_{n=0}^{n_{\text{cut}}} p_{n|j} e_{j,n}^Z, \\ E_j^Z \leqslant \sum_{n=0}^{n_{\text{cut}}} p_{n|j} e_{j,n}^Z + 1 - \sum_{n=0}^{n_{\text{cut}}} p_{n|j}, \end{cases} \tag{17}$$

for $j \in \{\text{s}, \text{d}, \text{v}\}$. Setting a threshold photon number n_{cut} as we do allows to define finite linear programs to estimate the single-photon yield and the single-photon error probability of the signal intensity window (i.e. the one devoted to key extraction).

Note that the Fock states $\sigma_{j,n}^Z$ and $\sigma_{x,j,n}$ are (generally) different for each setting j, and thus distinguishable for Eve. This implies that the yields $y_{j,n}^Z$ and the error probabilities $e_{j,n}^Z$ might be setting-dependent. As a consequence, it is mandatory to incorporate additional constraints in the decoy-state analysis. For this purpose, the tool that we use is the TD argument [36], presented in appendix C. This tool fundamentally limits the maximum bias that Eve may induce between the measurement statistics of two non-orthogonal quantum states, thus naturally providing upper bounds on the differences $|y_{j,n}^Z - y_{k,n}^Z|$ and $|e_{j,n}^Z - e_{k,n}^Z|$ for all $j, k \in \{\text{s}, \text{d}, \text{v}\}$ ($j \neq k$) and $n \in \mathbb{N}$. If we denote these bounds respectively as $\Delta_{j,k,n}^Z$ and $\tilde{\Delta}_{j,k,n}^Z$, the resulting linear programs that fulfil the decoy-state method read

$$\begin{aligned} \min \quad & y_{\text{s},1}^Z \\ \text{s.t.} \quad & Q_j^Z \geqslant \sum_{n=0}^{n_{\text{cut}}} p_{n|j} y_{j,n}^Z \ (j \in \{\text{s}, \text{d}, \text{v}\}), \\ & Q_j^Z \leqslant \sum_{n=0}^{n_{\text{cut}}} p_{n|j} y_{j,n}^Z + 1 - \sum_{n=0}^{n_{\text{cut}}} p_{n|j} \ (j \in \{\text{s}, \text{d}, \text{v}\}), \\ & \left| y_{j,n}^Z - y_{k,n}^Z \right| \leqslant \Delta_{j,k,n}^Z \ (j, k \in \{\text{s}, \text{d}, \text{v}\},\ j \neq k,\ n = 0, \ldots, n_{\text{cut}}), \\ & 0 \leqslant y_{j,n}^Z \leqslant 1 \ (j \in \{\text{s}, \text{d}, \text{v}\},\ n = 0, \ldots, n_{\text{cut}}), \end{aligned} \tag{18}$$

for the signal-setting single-photon yield, and

$$\begin{aligned} \max \quad & e_{\text{s},1}^Z \\ \text{s.t.} \quad & E_j^Z \geqslant \sum_{n=0}^{n_{\text{cut}}} p_{n|j} e_{j,n}^Z \ (j \in \{\text{s}, \text{d}, \text{v}\}), \\ & E_j^Z \leqslant \sum_{n=0}^{n_{\text{cut}}} p_{n|j} e_{j,n}^Z + 1 - \sum_{n=0}^{n_{\text{cut}}} p_{n|j} \ (j \in \{\text{s}, \text{d}, \text{v}\}), \\ & \left| e_{j,n}^Z - e_{k,n}^Z \right| \leqslant \tilde{\Delta}_{j,k,n}^Z \ (j, k \in \{\text{s}, \text{d}, \text{v}\},\ j \neq k,\ n = 0, \ldots, n_{\text{cut}}), \\ & 0 \leqslant e_{j,n}^Z \leqslant 1 \ (j \in \{\text{s}, \text{d}, \text{v}\},\ n = 0, \ldots, n_{\text{cut}}), \end{aligned} \tag{19}$$

for the signal-setting single-photon error probability.

Importantly, replacing Z by X everywhere above, the relevant quantities —Q_j^X, E_j^X, $y_{j,n}^X$, $e_{j,n}^X$, $\Delta_{j,k,n}^X$ and $\tilde{\Delta}_{j,k,n}^X$— and linear programs for the X basis follow. Coming next, we compute the specific values of $\Delta_{j,k,n}^Z$, $\Delta_{j,k,n}^X$, $\tilde{\Delta}_{j,k,n}^Z$ and $\tilde{\Delta}_{j,k,n}^X$ using the TD argument.

4.1. Calculation of $\Delta_{j,k,n}^Z$ and $\Delta_{j,k,n}^X$

For simplicity of the notation, the derivation below assumes collective attacks. Nevertheless, explicit calculation easily shows that the resulting bounds hold against fully general attacks too. This feature follows from the tensor product structure of the global state of all protocol rounds.

Let $\hat{U}_{\mathrm{BE}}$ denote Eve's unitary operation in any given round, acting on the system B transmitted through the channel and a probe system E under Eve's control, initialized in a certain state $|\varphi\rangle_{\mathrm{E}}$. Also, for the purpose of evaluating the yields, Bob's possible measurement outcomes are either 'click' or 'no click'. Therefore, his Z basis measurement is described by a positive-operator-valued measure (POVM) with elements $\{\hat{M}_{\mathrm{B}}^{\mathrm{click}}, \hat{M}_{\mathrm{B}}^{\mathrm{no\,click}}\}$, where $\hat{M}_{\mathrm{B}}^{\mathrm{no\,click}} = \mathbb{1}_{\mathrm{B}} - \hat{M}_{\mathrm{B}}^{\mathrm{click}}$. Note that we are assuming the basis-independent detection efficiency condition here, such that no basis dependence is included in the POVM elements.

Now, recalling that $y_{j,n}^Z = p\left(\mathrm{click}|\sigma_{j,n}^Z, Z\right)$, it follows that

$$y_{j,n}^Z = \mathrm{Tr}\left[\hat{U}_{\mathrm{BE}}^\dagger \hat{M}_{\mathrm{B}}^{\mathrm{click}} \hat{U}_{\mathrm{BE}}\left(\sigma_{j,n}^Z \otimes |\varphi\rangle\langle\varphi|_{\mathrm{E}}\right)\right] \tag{20}$$

for all $j \in \{\mathrm{s}, \mathrm{d}, \mathrm{v}\}$ and $n \in \mathbb{N}$. Note that, aiming to keep the notation introduced in section 2, the subscript B of Bob's system is not made explicit in the state between brackets. From equation (20), direct application of the TD argument (see appendix C) yields

$$\left|y_{j,n}^Z - y_{k,n}^Z\right| \leqslant D\left(\sigma_{j,n}^Z, \sigma_{k,n}^Z\right) \tag{21}$$

for all $j, k \in \{\mathrm{s}, \mathrm{d}, \mathrm{v}\}$ and $n \in \mathbb{N}$, where

$$D\left(\sigma_{j,n}^Z, \sigma_{k,n}^Z\right) = \frac{1}{2}\mathrm{Tr}\left[\sqrt{\left(\sigma_{j,n}^Z - \sigma_{k,n}^Z\right)^2}\right] = \Delta_{j,k,n}^Z \tag{22}$$

is the TD between $\sigma_{j,n}^Z$ and $\sigma_{k,n}^Z$.

A similar procedure leads to $\Delta_{j,k,n}^X = D\left(\sigma_{j,n}^X, \sigma_{k,n}^X\right)$, and in virtue of the azimuthal symmetry it follows that $\Delta_{j,k,n}^X = \Delta_{j,k,n}^Z$ for all possible inputs. To finish with, we remark that evaluating the TD values $\Delta_{j,k,n}^Z$ requires to provide a matrix representation of the input density matrices. In this regard, a natural representation is given in appendix D.

4.2. Calculation of $\tilde{\Delta}_{j,k,n}^Z$ and $\tilde{\Delta}_{j,k,n}^X$

For the purpose of evaluating the Z basis error probabilities, finer-grained measurement operators are required, in a one-to-one correspondence with Bob's possible outcomes '0', 'π' and 'no click' (as usual, double clicks are randomly assigned to a detection event, i.e. '0' or 'π' in this case). Therefore, error-wise, Bob's measurement is described by a POVM with elements $\{\hat{M}_{\mathrm{B}}^0, \hat{M}_{\mathrm{B}}^\pi, \hat{M}_{\mathrm{B}}^{\mathrm{no\,click}}\}$, where $\hat{M}_{\mathrm{B}}^0 + \hat{M}_{\mathrm{B}}^\pi = \hat{M}_{\mathrm{B}}^{\mathrm{click}}$.

Recalling that $e_{j,n}^Z = p\left(\mathrm{err}|\sigma_{j,n}^Z, Z\right)$ and that $\sigma_{j,n}^Z = \left(\sigma_{0,j,n} + \sigma_{\pi,j,n}\right)/2$, it follows that

$$\begin{aligned} e_{j,n}^Z &= \frac{1}{2}\left[p\left(\mathrm{err}|\sigma_{0,j,n}, Z\right) + p\left(\mathrm{err}|\sigma_{\pi,j,n}, Z\right)\right] \\ &= \frac{1}{2}\left\{\mathrm{Tr}\left[\hat{U}_{\mathrm{BE}}^\dagger \hat{M}_{\mathrm{B}}^\pi \hat{U}_{\mathrm{BE}}\left(\sigma_{0,j,n} \otimes |\varphi\rangle\langle\varphi|_{\mathrm{E}}\right)\right] + \mathrm{Tr}\left[\hat{U}_{\mathrm{BE}}^\dagger \hat{M}_{\mathrm{B}}^0 \hat{U}_{\mathrm{BE}}\left(\sigma_{\pi,j,n} \otimes |\varphi\rangle\langle\varphi|_{\mathrm{E}}\right)\right]\right\} \end{aligned} \tag{23}$$

for all $j \in \{\mathrm{s}, \mathrm{d}, \mathrm{v}\}$ and $n \in \mathbb{N}$. That is to say, upon post-selection of $\sigma_{0,j,n}$ ($\sigma_{\pi,j,n}$), an error occurs if Bob records the outcome 'π' ('0'). Hence, defining $e_{0,j,n} = p\left(\mathrm{err}|\sigma_{0,j,n}, Z\right)$ and $e_{\pi,j,n} = p\left(\mathrm{err}|\sigma_{\pi,j,n}, Z\right)$, the TD argument provides the constraints

$$|e_{0,j,n} - e_{0,k,n}| \leqslant D\left(\sigma_{0,j,n}, \sigma_{0,k,n}\right) \quad \text{and} \quad |e_{\pi,j,n} - e_{\pi,k,n}| \leqslant D\left(\sigma_{\pi,j,n}, \sigma_{\pi,k,n}\right) \tag{24}$$

for all $j, k \in \{\mathrm{s}, \mathrm{d}, \mathrm{v}\}$ and $n \in \mathbb{N}$. From equation (24) and the triangle inequality, the desired bound on the bias $|e_{j,n}^Z - e_{k,n}^Z|$ follows. Namely,

$$\left|e^Z_{j,n}-e^Z_{k,n}\right| \leqslant \frac{1}{2}\left[D\left(\sigma_{0,j,n},\sigma_{0,k,n}\right)+D\left(\sigma_{\pi,j,n},\sigma_{\pi,k,n}\right)\right] \tag{25}$$

for all $j,k\in\{\mathrm{s},\mathrm{d},\mathrm{v}\}$ and $n\in\mathbb{N}$. In conclusion, $\tilde{\Delta}^Z_{j,k,n}=\left[D\left(\sigma_{0,j,n},\sigma_{0,k,n}\right)+D\left(\sigma_{\pi,j,n},\sigma_{\pi,k,n}\right)\right]/2$. What is more, the azimuthal symmetry assures that $D\left(\sigma_{0,j,n},\sigma_{0,k,n}\right)=D\left(\sigma_{\pi,j,n},\sigma_{\pi,k,n}\right)$, and thus

$$\tilde{\Delta}^Z_{j,k,n}=D\left(\sigma_{0,j,n},\sigma_{0,k,n}\right). \tag{26}$$

Again, proceeding identically and invoking the symmetry, for the X basis one finds $\tilde{\Delta}^X_{j,k,n}=D\left(\sigma_{\frac{\pi}{2},j,n},\sigma_{\frac{\pi}{2},k,n}\right)=D\left(\sigma_{0,j,n},\sigma_{0,k,n}\right)=\tilde{\Delta}^Z_{j,k,n}$ for all possible inputs. As before, the reader is referred to appendix D for a matrix representation of the $\sigma_{x,j,n}$, necessary for the calculation of the TD values $\tilde{\Delta}^Z_{j,k,n}$.

5. Entanglement-based protocol and single-photon phase-error rate

As in the previous section, we assume the restricted scenario of collective attacks, and recall that this suffices to establish a valid asymptotic key rate analysis against coherent attacks in virtue of the de Finetti theorem [37] or the post-selection technique [38].

Throughout this section, we shall only refer to the single-photon component $\sigma_{x,\mathrm{s},1}$ of the output states $\sigma_{x,\mathrm{s}}$ (see equation (15)), where we recall that we set $j=\mathrm{s}$ because we assume that the key is extracted from the signal intensity window, I_s. For convenience, we define $|\mathrm{R}\rangle=a^\dagger_\mathrm{R}|\mathrm{vac}\rangle$ and $|\mathrm{L}\rangle=a^\dagger_\mathrm{L}|\mathrm{vac}\rangle$ (poles of the RL Bloch sphere).

The formulation of the virtual entanglement-based (EB) protocol proceeds in two steps. In a first step, we consider a purification of $\sigma_{x,\mathrm{s},1}$ via a shield qubit system A inaccessible to all Alice, Bob and Eve. In particular, this requires diagonalizing $\sigma_{x,\mathrm{s},1}$ first. In a second step, we consider an additional purification via an ancillary system A' held by Alice, which determines the states she prepares for Bob via projective measurements as usual. Bob's system shall be denoted by the subscript B.

For the purpose of diagonalizing $\sigma_{x,\mathrm{s},1}=\langle e^{-I}I|1\rangle\langle 1|_{\theta,\phi}\rangle_{\Omega_{x,\mathrm{s}}}/\langle e^{-I}I\rangle_{\Omega_{x,\mathrm{s}}}$, we use again the matrix representation provided in appendix D. In particular, from equation (D7), straightforward algebra leads to

$$\sigma_{x,\mathrm{s},1}=\frac{\mathbb{1}_\mathrm{B}}{2}+\Delta_\mathrm{s}\left(e^{ix}|\mathrm{L}\rangle\langle\mathrm{R}|_\mathrm{B}+e^{-ix}|\mathrm{R}\rangle\langle\mathrm{L}|_\mathrm{B}\right) \tag{27}$$

in the orthonormal basis $\{|\mathrm{R}\rangle,|\mathrm{L}\rangle\}$, where $\mathbb{1}_\mathrm{B}$ denotes the identity operator and

$$\Delta_\mathrm{s}=\frac{\sin(\Delta\phi)}{2\Delta\phi}\times\frac{\displaystyle\int_{\frac{\pi}{2}-\Delta\theta}^{\frac{\pi}{2}+\Delta\theta}\mathrm{d}\theta\sin\theta\int_{I_\mathrm{s}}\mathrm{d}I f_{\boldsymbol{\theta},I}(\theta,I)e^{-I}I}{\displaystyle\int_{\frac{\pi}{2}-\Delta\theta}^{\frac{\pi}{2}+\Delta\theta}\mathrm{d}\theta\int_{I_\mathrm{s}}\mathrm{d}I f_{\boldsymbol{\theta},I}(\theta,I)e^{-I}I}. \tag{28}$$

Naturally, $\sigma_{x,\mathrm{s},1}$ is diagonal in the $\{|x\rangle_\mathrm{B},|x+\pi\rangle_\mathrm{B}\}$ basis, where $|x\rangle_\mathrm{B}=\frac{1}{\sqrt{2}}\left(|\mathrm{R}\rangle_\mathrm{B}+e^{ix}|\mathrm{L}\rangle_\mathrm{B}\right)$. Note that $|x\rangle_\mathrm{B}$ is a pure state in the RL Bloch sphere with $\theta=\pi/2$ and $\phi=x$. In particular, explicit diagonalization yields

$$\sigma_{x,\mathrm{s},1}=\left(\frac{1}{2}+\Delta_\mathrm{s}\right)|x\rangle\langle x|_\mathrm{B}+\left(\frac{1}{2}-\Delta_\mathrm{s}\right)|x+\pi\rangle\langle x+\pi|_\mathrm{B}, \tag{29}$$

such that after attaching the shield system A —with, say, orthonormal basis $\{|0\rangle_\mathrm{A},|\pi\rangle_\mathrm{A}\}$—, the purified state reads

$$|\Psi_{x,\mathrm{s},1}\rangle_\mathrm{AB}=\sum_{\delta\in\{0,\pi\}}\left(\frac{1}{2}+e^{i\delta}\Delta_\mathrm{s}\right)^{1/2}|\delta\rangle_\mathrm{A}|x+\delta\rangle_\mathrm{B}. \tag{30}$$

As stated above, in the virtual EB approach Alice holds an ancillary polarization qubit A' maximally entangled to Bob's purified qubit AB. That is to say, whenever Ω^Z_s is post-selected and a single-photon is emitted, the equivalent three-partite state prepared by Alice in the EB protocol reads

$$|\Psi_{s,1}\rangle_{A'AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_{A'}|\Psi_{0,s,1}\rangle_{AB} + |\pi\rangle_{A'}|\Psi_{\pi,s,1}\rangle_{AB}\right), \tag{31}$$

where again we are using the RL Bloch sphere notation $|y\rangle_{A'} = \frac{1}{\sqrt{2}}\left(|R\rangle_{A'} + e^{iy}|L\rangle_{A'}\right)$. Importantly, it is shown in appendix E that equation (31) can be rewritten as

$$|\Psi_{s,1}\rangle_{A'AB} = \frac{1}{\sqrt{2}}\left(\left|\frac{\pi}{2}\right\rangle_{A'}\left|\Psi_{-\frac{\pi}{2},s,1}\right\rangle_{AB} + \left|-\frac{\pi}{2}\right\rangle_{A'}\left|\Psi_{\frac{\pi}{2},s,1}\right\rangle_{AB}\right). \tag{32}$$

Therefore, the Z basis phase-error probability ϕ_s^Z is defined as the bit-error probability between the outcomes $\mathbf{X}_{A'}$ and $\mathbf{X}_B$, reached by measuring the polarization qubits A′ and B in the test bases [39] (i.e. $\{|\pi/2\rangle\langle\pi/2|_{A'}, |-\pi/2\rangle\langle-\pi/2|_{A'}\}$ and $\{|\pi/2\rangle\langle\pi/2|_B, |-\pi/2\rangle\langle-\pi/2|_B\}$, respectively). In the prepare-and-measure picture, this matches the bit-error probability that arises when Ω_s^X is post-selected, a single-photon is emitted (these two features are equivalent to asserting that $\sigma_{s,1}^X$ is post-selected), and Bob selects the X basis. Namely,

$$\phi_s^Z = \frac{p\left(\text{err}|\sigma_{s,1}^X, X\right)}{p\left(\text{click}|\sigma_{s,1}^X, X\right)} = \frac{e_{s,1}^X}{y_{s,1}^X}. \tag{33}$$

As usual, one can define the X basis single-photon phase-error probability ϕ_s^X in an entirely identical fashion, and it can be computed as $\phi_s^X = e_{s,1}^Z/y_{s,1}^Z$ following the same argument presented here.

6. Performance

The secret key rate formula of our passive QKD scheme is determined by the fact that we consider a decoy-state BB84 protocol, with the minor difference that one must deal with the continuous post-selection regions introduced by the PT.

Naturally, we assume that both bases are used for key extraction, because they are equally likely to be post-selected. In short, the secret key rate reads $K = K_Z + K_X$ with

$$K_M = q_M \times \left\{\left\langle e^{-I}I\right\rangle_{\Omega_s^M} y_{s,1}^M\left[1 - h\left(\phi_s^M\right)\right] - f_{EC}\left\langle 1\right\rangle_{\Omega_s^M} Q_s^M h\left(\frac{E_s^M}{Q_s^M}\right)\right\}, \tag{34}$$

where $M \in \{Z, X\}$, q_M stands for Bob's probability to select basis M ($q_M = 1/2$ being optimal for symmetry reasons), $h(\cdot)$ stands for Shannon's binary entropy function, and f_{EC} denotes the error correction efficiency.

In what follows, we evaluate the rate-distance performance of the PT illustrated in figure 2. For this purpose, in the absence of experimental data, we consider a natural channel and detector model presented in appendix F. The model is specified by the channel transmittance, $\eta_{ch} = 10^{-\alpha_{att}L/10}$ —where α_{att} denotes the attenuation coefficient of the channel and L stands for its transmission length—, the detector efficiency of Bob's detectors, η_{Bob}, and their dark count rate, p_d. For illustration purposes, we set these parameters to typical values of $\alpha_{att} = 0.2$ dB km^{-1} (telecom wavelength attenuation), $\eta_{Bob} = 65\%$ and $p_d = 10^{-6}$. As for the input settings of the PT, we assume that no intensity value in the accessible range $(0, 4\nu t)$ is withdrawn, such that the intervals I_v, I_d and I_s are strictly consecutive and exhaustive in this range. Also, we fix the width of $I_v/4\nu t$ and $I_d/4\nu t$ to a reasonable small value of 5×10^{-3} for the numerics. Hence, $I_v/4\nu t = (0, 5) \times 10^{-3}$ and $I_d/4\nu t = (5, 10) \times 10^{-3}$. The product νt and the angular widths $\Delta\theta$ and $\Delta\phi$ of the post-selection regions are numerically optimized to maximize the secret key rate for each value of L, and the optimization reveals a roughly constant optimal value $\nu t \approx 0.25$. Finally, we set the threshold photon number for the decoy-state linear programs to $n_{cut} = 3$. Importantly, the loss of generality of the above numerical specifications is very small, as we check that the delivered secret key rate is remarkably close to the perfect decoy-state parameter estimation limit (which we compute under full optimization as well). The results are shown in figure 4, where we further include the secret key rate reached in the active setting for comparison purposes.

The figure shows that the security and simplicity upgrades of the PT come at the price of lowering the secret key rate by a factor $\sim 1/20$. As mentioned in section 1, the origin of this discrepancy is twofold. In the first place, the post-selection of acceptance regions requires additional sifting compared to the active setting. In the second place, the post-selected $\sigma_{x,j,n}$ are in a mixed polarization state. This represents an inherent source of noise not present in the active case, where one typically considers pure states with fixed polarizations.

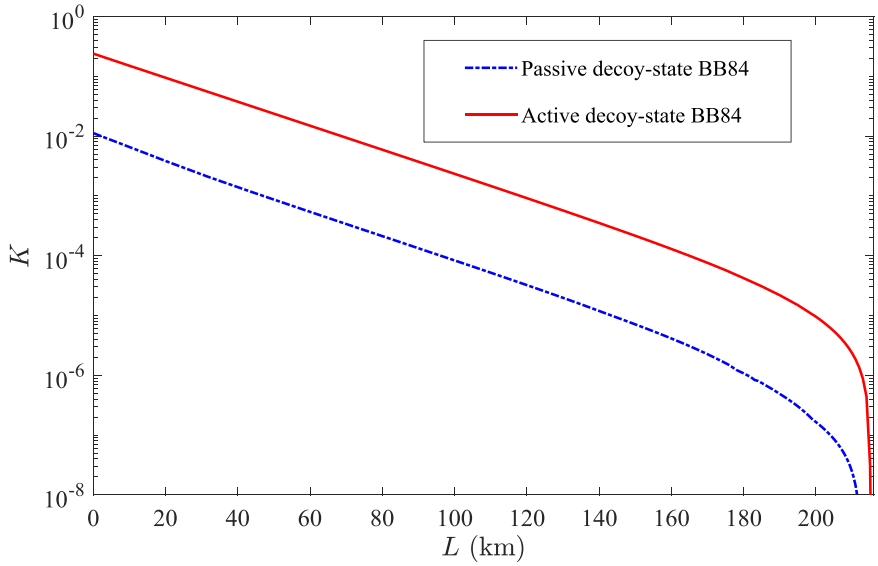

Figure 4. Rate-distance performance of our fully passive decoy-state BB84 proposal. For the sake of comparison, we include the secret key rate attained in the active setting as well (solid red line). The experimental parameters are set as specified in the main text.

7. Discussion

Active QKD systems often rely on the use of externally driven modulators, whose imperfections lead to security loopholes and side-channels (e.g. THAs), and whose frequency of operation typically limits the repetition rate of the system. Therefore, replacing all externally driven elements by a passive mechanism could be a very appealing feature for QKD: it provides immunity to modulator side channels and, in principle, it enables the operation of QKD systems at higher repetition rates. On top of it, passive architectures could reduce the complexity (and thereby the cost) of QKD infrastructures. Needless to say, this would entail an advantage in many practical situations, for instance, when it comes to deploying QKD on a satellite.

Despite the intense research in the field, working out a fully passive linear-optics setup for the celebrated decoy-state BB84 protocol remained an open problem for more than a decade. Nonetheless, the present work, together with that in [35], elucidate this possibility for the first time, and explicitly construct different fully passive protocols with very diverse approaches to polarization encoding and decoy-state parameter estimation. This clearly illustrates the versatility of the considered prototype. On top of it, we provide a detailed security analysis for the mixed single-photon states generated by the transmitter, tightening a loose end present in [35].

For implementation purposes, we remark that the usage of four independent lasers in the PT is not a necessity by any means, but rather an instrument we use for theoretical convenience. Identically as in [35] —where a detailed discussion is included—, the same physical states can be generated by using a single laser and suitable Mach–Zehnder interferometry. This configuration benefits from an enhanced simplicity, because high-visibility interference demands photon indistinguishability, which is typically hard to enforce when using independent lasers.

Furthermore, despite the resilience to modulator side-channels or THAs, certain other vulnerabilities may affect a PT. For instance, Eve could try to perform a laser-seeding attack to modify the phase/intensity of the laser pulses generated in the PT [40–42]. Attacks of this kind, known to threaten actively modulated systems too, could invalidate the estimation of the secret key length in the passive scenario. What is more, in the case of a PT, Eve could launch a laser-seeding attack to alter the measurement outcome of its photo-detection system. To counter these problems, optical isolation must be incorporated at the output port of the transmitter, as it is done to protect active systems against attacks that inject light from the channel (like e.g. THAs). Notwithstanding, current security proofs against THAs in the active setting typically require the intensity of the back-reflected light to be minuscule for the information leakage to be irrelevant (as an example, the analyses in [10–12] demand such intensity to lie below 10^{-7} or 10^{-8} photons/pulse). In contrast to this, much less isolation is expected to be required to deal with laser-seeding attacks in the PT. This is so because 'classical' (high intensity) light pulses are generated in the PT and arrive at Alice's measurement unit, say, containing 10^{6}–10^{8} photons/signal. Therefore, as long as the intensity of the injected light is attenuated well below this level, its effect on the generated pulses or on the reading of the detection scheme will probably

be negligible. Moreover, any slight modification of the actual measurement outcome due to Eve's action could be readily incorporated in the security proof. Similarly, laser-damage attacks [43] —which, again, have been proposed against active systems— may as well jeopardize the security of the PT. An attack of this kind might try to reduce the optical isolation of the transmitter, or to manipulate the behaviour of its internal components. As in the active setting, protection against laser-damage may be achieved with optical isolators, circulators, filters or even an optical fuse [44, 45]. In any case, a detailed analysis of these and other potential attacks where Eve actively meddles with the hardware lies beyond the scope of this work.

Leaving active tampering aside, potential information leakage via back-flash emission from the detection system might be another weakness of a PT that deserves further experimental investigation. If needed, this could probably be circumvented by simply using an anti-reflective coating. Also, we remark that Alice's intensity and polarization measurements are presumed to be noiseless in our analysis. However, to provide protection against a noisy measurement, the noise must be characterized to a certain extent because it affects the post-selected light pulses. Once characterized, it could be incorporated to the security analysis using similar techniques as it is done in the active setting to deal with e.g. state preparation flaws or intensity fluctuations.

After these various pending tasks are properly addressed, passive schemes could play a crucial role in the development of practical and affordable QKD solutions, in view of the increasing concerns related to the implementation security of QKD. This being the case, the present work is a valuable input to the topic.

Data availability statement

No new data were created or analysed in this study.

Acknowledgments

All authors gratefully acknowledge Chengqiu Hu for useful discussions. V Z and M C acknowledge 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 Grant No. PID2020-118178RB-C21, Cisco Systems Inc. and MICINN —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 Autonomas' in Quantum Communication. W W is supported by the University of Hong Kong Seed Fund for Basic Research for New Staff and the Hong Kong RGC General Research Fund.

Appendix A. Calculation of the pure output state of the transmitter

Here, we derive equations (2) and (3) using elementary quantum optics. Let us consider, say, the top arm of the PT in figure 2. Given $\nu \in \mathbb{R}^+$, $\alpha \in [0, 2\pi)$ and $\beta \in [0, 2\pi)$, the input state of the 50:50 beamsplitter (BS) reads

$$|\varphi_{\rm in}\rangle_{ab} = \left|\sqrt{\nu}e^{i\alpha}\right\rangle_{a,{\rm R}} \left|\sqrt{\nu}e^{i\beta}\right\rangle_{b,{\rm R}} = \exp\left\{\sqrt{\nu}e^{i\alpha}a_{\rm R}^\dagger - \sqrt{\nu}e^{-i\alpha}a_{\rm R}\right\} \times \exp\left\{\sqrt{\nu}e^{i\beta}b_{\rm R}^\dagger - \sqrt{\nu}e^{-i\beta}b_{\rm R}\right\}|{\rm vac}\rangle\,, \tag{A1}$$

and the unitary transformation of the BS is given by $\left\{a_{\rm R}^\dagger \to \frac{1}{\sqrt{2}}\left(c_{\rm R}^\dagger + d_{\rm R}^\dagger\right),\ b_{\rm R}^\dagger \to \frac{1}{\sqrt{2}}\left(d_{\rm R}^\dagger - c_{\rm R}^\dagger\right)\right\}$. This leads to

$$|\varphi_{\rm out}\rangle_{cd} = \exp\left\{\sqrt{\nu}\left(\frac{e^{i\alpha}-e^{i\beta}}{\sqrt{2}}c_{\rm R}^\dagger - \frac{e^{-i\alpha}-e^{-i\beta}}{\sqrt{2}}c_{\rm R}\right)\right\} \times \exp\left\{\sqrt{\nu}\left(\frac{e^{i\alpha}+e^{i\beta}}{\sqrt{2}}d_{\rm R}^\dagger - \frac{e^{-i\alpha}+e^{-i\beta}}{\sqrt{2}}d_{\rm R}\right)\right\}|{\rm vac}\rangle \tag{A2}$$

in the output modes c and d, after regrouping terms. Since mode d is not used, from now on we focus on mode c, and refer to the corresponding state in equation (A2) as $|\varphi_{\rm out}\rangle_c$. Factoring $\left(e^{i\alpha}-e^{i\beta}\right)/\sqrt{2}$ into modulus and phase yields $\left|\left(e^{i\alpha}-e^{i\beta}\right)/\sqrt{2}\right| = \sqrt{1-\cos(\beta-\alpha)}$ and

$$\begin{aligned}{\rm Arg}\left(\frac{e^{i\alpha}-e^{i\beta}}{\sqrt{2}}\right) &= \frac{e^{i\alpha}-e^{i\beta}}{\sqrt{2\left[1-\cos(\beta-\alpha)\right]}} = \frac{\cos\alpha-\cos\beta}{2\sin\left(\frac{\beta-\alpha}{2}\right)} + i\frac{\sin\alpha-\sin\beta}{2\sin\left(\frac{\beta-\alpha}{2}\right)} \\ &= \sin\left(\frac{\alpha+\beta}{2}\right) - i\cos\left(\frac{\alpha+\beta}{2}\right) = e^{i\left(\frac{\alpha+\beta}{2}-\frac{\pi}{2}\right)},\end{aligned} \tag{A3}$$

where the identity $\sqrt{2\left[1-\cos(\beta-\alpha)\right]}=2\left|\sin\left(\frac{\beta-\alpha}{2}\right)\right|=2\sin\left(\frac{\beta-\alpha}{2}\right)$ is used in the second equality, and the identities $\cos\alpha-\cos\beta=2\sin\left(\frac{\alpha+\beta}{2}\right)\sin\left(\frac{\beta-\alpha}{2}\right)$ and $\sin\alpha-\sin\beta=-2\cos\left(\frac{\alpha+\beta}{2}\right)\sin\left(\frac{\beta-\alpha}{2}\right)$ are used in the third equality. Putting it all together,

$$\begin{aligned}|\varphi_{\text{out}}\rangle_c &= \exp\left\{\sqrt{\nu\left[1-\cos(\beta-\alpha)\right]}\left[e^{i\left(\frac{\alpha+\beta}{2}-\frac{\pi}{2}\right)}c_{\text{R}}^{\dagger}-e^{-i\left(\frac{\alpha+\beta}{2}-\frac{\pi}{2}\right)}c_{\text{R}}\right]\right\}|\text{vac}\rangle\\ &= \left|\sqrt{\nu\left[1-\cos(\beta-\alpha)\right]}e^{i\left(\frac{\alpha+\beta}{2}-\frac{\pi}{2}\right)}\right\rangle_{c,\text{R}}.\end{aligned} \tag{A4}$$

Similarly, the output state of the bottom arm in mode r reads $|\psi_{\text{out}}\rangle_r=\left|\sqrt{\nu\left[1-\cos(\delta-\gamma)\right]}e^{i\left(\frac{\gamma+\delta}{2}-\frac{\pi}{2}\right)}\right\rangle_{r,\text{L}}$.

Next, $|\varphi_{\text{out}}\rangle_c$ and $|\psi_{\text{out}}\rangle_r$ interfere at a polarizing BS (PBS) that maps $c_{\text{R}}^{\dagger}$ to $v_{\text{R}}^{\dagger}$ and $r_{\text{L}}^{\dagger}$ to $v_{\text{L}}^{\dagger}$. Explicit calculation shows that the output state of the PBS at mode v reads

$$|\Upsilon\rangle_v=\exp\left\{\sqrt{\nu_{\alpha\beta}+\nu_{\gamma\delta}}\,e^{i\tau_{\alpha\beta}}\left[\sqrt{\frac{\nu_{\alpha\beta}}{\nu_{\alpha\beta}+\nu_{\gamma\delta}}}v_{\text{R}}^{\dagger}+\sqrt{\frac{\nu_{\gamma\delta}}{\nu_{\alpha\beta}+\nu_{\gamma\delta}}}e^{i(\tau_{\gamma\delta}-\tau_{\alpha\beta})}v_{\text{L}}^{\dagger}\right]-\widehat{\text{h.c.}}\right\}|\text{vac}\rangle\,, \tag{A5}$$

where we have defined $\nu_{\rho\sigma}=\nu\left[1-\cos(\sigma-\rho)\right]$ and $\tau_{\rho\sigma}=\frac{\rho+\sigma}{2}-\frac{\pi}{2}$ for $\rho\in[0,2\pi)$ and $\sigma\in[0,2\pi)$. Also, we introduce the shorthand notation '$\widehat{\text{h.c.}}$' to denote the hermitian conjugate of the first term between keys.

Equation (A5) triggers the definition of $I'=\nu_{\alpha\beta}+\nu_{\gamma\delta}$, $\psi=\tau_{\alpha\beta}$ and $\theta\in[0,\pi]$, $\phi\in[0,2\pi)$ such that $\frac{\theta}{2}=\arctan\sqrt{\nu_{\gamma\delta}/\nu_{\alpha\beta}}$ and $\phi=\tau_{\gamma\delta}-\tau_{\alpha\beta}$. In terms of I', ψ, θ and ϕ, $|\Upsilon\rangle_v$ reads

$$\begin{aligned}|\Upsilon\rangle_v &= \exp\left\{\sqrt{I'}e^{i\psi}\left[\cos\left(\frac{\theta}{2}\right)v_{\text{R}}^{\dagger}+\sin\left(\frac{\theta}{2}\right)e^{i\phi}v_{\text{L}}^{\dagger}\right]-\widehat{\text{h.c.}}\right\}|\text{vac}\rangle\\ &= \exp\left\{\sqrt{I'}e^{i\psi}v_{\theta,\phi}^{\dagger}-\widehat{\text{h.c.}}\right\}|\text{vac}\rangle=\left|\sqrt{I'}\,e^{i\psi}\right\rangle_{v,\theta,\phi},\end{aligned} \tag{A6}$$

where we recall that the notation $v_{\theta,\phi}^{\dagger}$ is presented in equation (1). Lastly, $|\Upsilon\rangle_v$ enters a BS with transmittance t, which maps $v_{\theta,\phi}^{\dagger}$ to $(\sqrt{t}\,w_{\theta,\phi}^{\dagger}+\sqrt{1-t}\,y_{\theta,\phi}^{\dagger})$. This trivially leads to the final output state $|\Psi\rangle_{wy}=\left|\sqrt{tI'}\,e^{i\psi}\right\rangle_{w,\theta,\phi}\left|\sqrt{(1-t)I'}\,e^{i\psi}\right\rangle_{y,\theta,\phi}$ in modes w and y. In particular, setting $I=tI'$, the state that is sent to the channel reads

$$|\Psi\rangle_w=\left|\sqrt{I}\,e^{i\psi}\right\rangle_{w,\theta,\phi}. \tag{A7}$$

Making the dependence on ν, α, β, γ, δ and t explicit, we see that

$$\begin{aligned}&I=\nu t\left[2-\cos(\beta-\alpha)-\cos(\delta-\gamma)\right]=2\nu t\left[\sin^2\left(\frac{\beta-\alpha}{2}\right)+\sin^2\left(\frac{\delta-\gamma}{2}\right)\right], \qquad \psi=\frac{\alpha+\beta}{2}-\frac{\pi}{2},\\ &\theta=2\arctan\sqrt{\frac{1-\cos(\delta-\gamma)}{1-\cos(\beta-\alpha)}}=2\arctan\left[\sin\left(\frac{\delta-\gamma}{2}\right)\Big/\sin\left(\frac{\beta-\gamma}{2}\right)\right] \quad \text{and} \quad \phi=\frac{\gamma+\delta}{2}-\frac{\alpha+\beta}{2},\end{aligned} \tag{A8}$$

where the first identity invoked in equation (A3) has been used again. Note that equations (A7) and (A8) respectively match equations (2) and (3) exactly, as we wanted to show.

Appendix B. Calculation of the output probability density function of the transmitter

In this appendix, we shall use bold letters to denote random variables (RVs). The starting point is the definition of the output RVs $\boldsymbol{\phi}$, $\boldsymbol{\theta}$ and $\boldsymbol{I}$ of the PT, given in equation (3):

$$\begin{aligned}\boldsymbol{\phi}&=\boldsymbol{\delta_2}+\frac{\boldsymbol{\delta_1}+\boldsymbol{\delta_3}}{2},\\ \boldsymbol{\theta}&=2\arctan\left[\sin\left(\frac{\boldsymbol{\delta_3}}{2}\right)\Big/\sin\left(\frac{\boldsymbol{\delta_1}}{2}\right)\right],\\ \boldsymbol{I}&=2\nu t\left[\sin^2\left(\frac{\boldsymbol{\delta_1}}{2}\right)+\sin^2\left(\frac{\boldsymbol{\delta_3}}{2}\right)\right].\end{aligned} \tag{B1}$$

B.1. Distribution and independence of ϕ

In the first place, since $\boldsymbol{\delta_1}$, $\boldsymbol{\delta_2}$ and $\boldsymbol{\delta_3}$ are independent and uniformly distributed in $[0,2\pi)$, it trivially follows that $\boldsymbol{\phi}$ is uniformly distributed in $[0,2\pi)$ too. Namely, $f_{\boldsymbol{\phi}}(\phi)=1/2\pi$ for all $\phi\in[0,2\pi)$. We discuss the independence of $\boldsymbol{\phi}$ from the bivariate RV $(\boldsymbol{\theta},\boldsymbol{I})$ next. In fact, it suffices to notice that, according to equation (B1), $\boldsymbol{\phi}\big|_{(\boldsymbol{\delta_1},\boldsymbol{\delta_3})=(\delta_1,\delta_3)}$ is of the form 'constant phase plus uniformly distributed phase', such that $f_{\boldsymbol{\phi}|(\boldsymbol{\delta_1},\boldsymbol{\delta_3})=(\delta_1,\delta_3)}(\phi)=1/2\pi=f_{\boldsymbol{\phi}}(\phi)$ for all δ_1, δ_3. This independence between $\boldsymbol{\phi}$ and $(\boldsymbol{\delta_1},\boldsymbol{\delta_3})$ straightforwardly implies the independence of $\boldsymbol{\phi}$ from $(\boldsymbol{\theta},\boldsymbol{I})$.

B.2. Distribution of θ and I

Here, we compute the joint PDF of $\boldsymbol{\theta}$ and $\boldsymbol{I}$, $f_{\boldsymbol{\theta},\boldsymbol{I}}$, and recall that $f_{\boldsymbol{\phi},\boldsymbol{\theta},\boldsymbol{I}}=f_{\boldsymbol{\phi}}\times f_{\boldsymbol{\theta},\boldsymbol{I}}$ in virtue of the previous discussion.

The starting point is the joint PDF of the independent variables $\boldsymbol{\delta_1}$ and $\boldsymbol{\delta_3}$ —given by $f_{\boldsymbol{\delta_1},\boldsymbol{\delta_3}}(\delta_1,\delta_3)=1/(2\pi)^2$ for all $(\delta_1,\delta_3)\in\mathcal{R}=[0,2\pi)\times[0,2\pi)$— and the function g that maps $(\boldsymbol{\delta_1},\boldsymbol{\delta_3})$ to $(\boldsymbol{\theta},\boldsymbol{I})$. For convenience, we shall deal with the dimensionless variable $\boldsymbol{y}=\boldsymbol{I}/2\nu t$, such that the relevant function G (identical to g up to a constant prefactor in the second component) reads

$$G:\begin{cases}\theta=2\arctan\left[\sin\left(\dfrac{\delta_3}{2}\right)\Big/\sin\left(\dfrac{\delta_1}{2}\right)\right]\\[2ex] y=\sin^2\left(\dfrac{\delta_1}{2}\right)+\sin^2\left(\dfrac{\delta_3}{2}\right).\end{cases}\tag{B2}$$

Despite the non-injectiveness of G in $\mathcal{R}$, G is symmetric with respect to the axes $\delta_1=\pi$ and $\delta_3=\pi$, and its restriction $G|_{Q_k}$ to any of the four quadrants Q_k of $\mathcal{R}$ defined by these axes is injective. Therefore, any (θ,y) in the interior of $G(\mathcal{R})$ accumulates the probability densities coming from all $G^{-1}(\theta,y)\cap Q_k$ (related with each other by reflections with respect to the axes), and in virtue of the bivariate transformation theorem it follows that

$$f_{\boldsymbol{\theta},\boldsymbol{y}}(\theta,y)=\sum_{k=1}^{4}f_{\boldsymbol{\delta_1},\boldsymbol{\delta_3}}\left(G^{-1}(\theta,y)\cap Q_k\right)\left|J_G\left(G^{-1}(\theta,y)\cap Q_k\right)\right|^{-1},\tag{B3}$$

where J_G is the Jacobian determinant of the G function,

$$J_G(\delta_1,\delta_3)=\det\begin{bmatrix}\dfrac{\partial\theta}{\partial\delta_1} & \dfrac{\partial\theta}{\partial\delta_3}\\[2ex] \dfrac{\partial y}{\partial\delta_1} & \dfrac{\partial y}{\partial\delta_3}\end{bmatrix}=-\cos\left(\frac{\delta_1}{2}\right)\cos\left(\frac{\delta_3}{2}\right).\tag{B4}$$

We remark that the r.h.s. in equation (B4) follows from explicit calculation of the derivatives and the determinant. Notably, $|J_G(\delta_1,\delta_3)|$ is invariant under reflections with respect to $\delta_1=\pi$ and/or $\delta_3=\pi$, such that $|J_G\left(G^{-1}(\theta,y)\cap Q_k\right)|$ in equation (B3) takes the same value for all four contributions to the preimage of (θ,y). Since, in addition, $f_{\boldsymbol{\delta_1},\boldsymbol{\delta_3}}(\delta_1,\delta_3)=1/(2\pi)^2$ for all pairs (δ_1,δ_3), equation (B3) simplifies as

$$f_{\boldsymbol{\theta},\boldsymbol{y}}(\theta,y)=\pi^{-2}\left|J_G\left(G^{-1}(\theta,y)\cap Q_1\right)\right|^{-1}.\tag{B5}$$

At the symmetry axes $\delta_1=\pi$ and $\delta_3=\pi$, which are necessarily mapped to the boundary of $G(\mathcal{R})$, $J_G(\delta_1,\delta_3)$ vanishes. As a consequence, $f_{\boldsymbol{\theta},\boldsymbol{y}}$ is divergent in this frontier. Note, however, that this feature does not compromise the normalization of $f_{\boldsymbol{\theta},\boldsymbol{y}}$ or the finiteness of any physical quantity relevant to the problem.

All that remains is to write down the Jacobian determinant of equation (B4) in terms of θ and y. In order to do this, it suffices to notice that

$$\cos^2\left(\frac{\theta}{2}\right)=\frac{\sin^2\left(\dfrac{\delta_1}{2}\right)}{\sin^2\left(\dfrac{\delta_1}{2}\right)+\sin^2\left(\dfrac{\delta_3}{2}\right)}\ \text{and}\ \sin^2\left(\frac{\theta}{2}\right)=\frac{\sin^2\left(\dfrac{\delta_3}{2}\right)}{\sin^2\left(\dfrac{\delta_1}{2}\right)+\sin^2\left(\dfrac{\delta_3}{2}\right)}\tag{B6}$$

in virtue of equation (B2), such that

$$1-y\cos^2\left(\frac{\theta}{2}\right)=\cos^2\left(\frac{\delta_1}{2}\right)\ \text{and}\ 1-y\sin^2\left(\frac{\theta}{2}\right)=\cos^2\left(\frac{\delta_3}{2}\right).\tag{B7}$$

Substituting these two relations in equation (B4) and plugging the result in equation (B5) yields

$$f_{\boldsymbol{\theta},\boldsymbol{y}}(\theta,y)=\frac{1}{\pi^2\sqrt{1-y\cos^2\left(\frac{\theta}{2}\right)}\sqrt{1-y\sin^2\left(\frac{\theta}{2}\right)}}. \tag{B8}$$

To finish with, let us explicitly identify the domain of $f_{\boldsymbol{\theta},\boldsymbol{y}}(\theta,y)$, given by the image of the domain $\mathcal{R}$ via G. In virtue of the symmetry of G, $G(\mathcal{R})=G(Q_k)$ for all k, and thus it suffices to show that G maps, say, the quadrant $Q_1=[0,\pi]\times[0,\pi]$ to the region

$$G(Q_1)=\left\{\theta\in[0,\pi],y\in[0,y_{\max,\theta}]\right\}, \tag{B9}$$

where $y_{\max,\theta}=\min\left\{1/\cos^2(\theta/2),1/\sin^2(\theta/2)\right\}$. For this purpose, we identify the image of the boundary of Q_1 via G, which certainly defines the boundary of $G(Q_1)$. If, for instance, we label the sides of the rectangle Q_1 as $L_1=\{\delta_1\in[0,\pi],\delta_3=0\}$, $L_2=\{\delta_1\in[0,\pi],\delta_3=\pi\}$, $L_3=\{\delta_1=0,\delta_3\in[0,\pi]\}$ and $L_4=\{\delta_1=\pi,\delta_3\in[0,\pi]\}$, one can readily show that L_1 contributes with the border $G(L_1)=\{\theta=0,y\in[0,1]\}$, L_2 with the border $G(L_2)=\{\theta\in[\pi/2,\pi],y=\sin(\theta/2)^{-2}\}$, L_3 with the border $G(L_3)=\{\theta=\pi,y\in[0,1]\}$ and L_4 with the border $G(L_4)=\{\theta\in[0,\pi/2],y=\cos(\theta/2)^{-2}\}$. These four borders (together with the defining constraint $y\geqslant 0$) shape the boundary of the region $G(Q_1)=G(\mathcal{R})$ defined in equation (B9).

Needless to say, $f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I)$ follows trivially from $f_{\boldsymbol{\theta},\boldsymbol{y}}(\theta,y)$ and the fact that $\boldsymbol{y}=\boldsymbol{I}/2\nu t$, leading to equation (8) in the main text (where the border $\{\theta\in[0,\pi],y=y_{\max,\theta}\}$ is excluded because of the divergence of $f_{\boldsymbol{\theta},\boldsymbol{I}}$).

Appendix C. Trace distance argument

Let ρ and σ be two density matrices of a quantum system of dimension d. The TD between them is defined as $D(\rho,\sigma)=\frac{1}{2}\mathrm{Tr}\left[\sqrt{(\rho-\sigma)^2}\right]$, and the TD argument states that $D(\rho,\sigma)=\max\left\{\mathrm{Tr}\left[\hat{O}(\rho-\sigma)\right]\right\}$, where the maximization is taken over all positive operators $\hat{O}\leqslant I$ [36].

Notably, from the definition of the TD it follows that $D(\rho,\sigma)=\sum_{i=1}^{d}|\lambda_i|$, where the λ_i are the eigenvalues of $\rho-\sigma$.

Appendix D. Numerical evaluation of the trace distance constraints

In order to evaluate the TD constraints of section 4, we express the Fock states $\sigma_{x,j,n}$ (defined in equation (15)) in a computational basis. For this purpose, we work with the unnormalized states

$$\tilde{\sigma}_{x,j,n}=\left\langle\frac{e^{-I}I^n}{n!}|n\rangle\langle n|_{\theta,\phi}\right\rangle_{\Omega_{x,j}} \tag{D1}$$

instead, and recall that $\sigma_{x,j,n}=\tilde{\sigma}_{x,j,n}/\mathrm{Tr}\left[\tilde{\sigma}_{x,j,n}\right]$ with $\mathrm{Tr}\left[\tilde{\sigma}_{x,j,n}\right]=\left\langle e^{-I}I^n/n!\right\rangle_{\Omega_{x,j}}$. The preferred basis that we use here is the one induced by the creation operators $a_{\mathrm{R}}^{\dagger}$ and $a_{\mathrm{L}}^{\dagger}$ presented in section 2:

$$\mathcal{B}_n=\left\{|n-k,k\rangle=\frac{a_{\mathrm{R}}^{\dagger n-k}a_{\mathrm{L}}^{\dagger k}}{\sqrt{(n-k)!k!}}|\mathrm{vac}\rangle\,,\ k=0,\ldots,n\right\}. \tag{D2}$$

Notably, $\mathcal{B}_n$ is an orthonormal basis of the Hilbert space $\mathcal{H}_n$ of n indistinguishable photons distributed across two modes, such that $\dim\mathcal{H}_n=n+1$. In particular, the states $|n\rangle\langle n|_{\theta,\phi}$ (defined in equation (6)) trivially decompose as

$$|n\rangle\langle n|_{\theta,\phi}=\sum_{k=0}^{n}\sum_{l=0}^{n}\sqrt{\binom{n}{k}\binom{n}{l}}e^{i(k-l)\phi}\cos^{2n-(k+l)}\left(\frac{\theta}{2}\right)\sin^{k+l}\left(\frac{\theta}{2}\right)|n-k,k\rangle\langle n-l,l| \tag{D3}$$

in virtue of Newton's binomial formula. Now, in contrast to the states $|n\rangle_{\theta,\phi}$, the basis elements $|n-k,k\rangle$ are independent of θ and ϕ, thereby allowing us to proceed with the angular integrals in

$$\left\langle\frac{e^{-I}I^n}{n!}|n\rangle\langle n|_{\theta,\phi}\right\rangle_{\Omega_{x,j}}=\frac{1}{2\pi}\int_{x-\Delta\phi}^{x+\Delta\phi}\mathrm{d}\phi\int_{\frac{\pi}{2}-\Delta\theta}^{\frac{\pi}{2}+\Delta\theta}\mathrm{d}\theta\int_{I_j}\mathrm{d}I f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I)\frac{e^{-I}I^n}{n!}|n\rangle\langle n|_{\theta,\phi}. \tag{D4}$$

Specifically, the relevant azimuthal integral in equation (D4) is given by

$$\frac{1}{2\pi}\int_{x-\Delta\phi}^{x+\Delta\phi} \mathrm{d}\phi e^{i(k-l)\phi} = \begin{cases} \dfrac{\Delta\phi}{\pi} & \text{if} \quad k=l, \\ \dfrac{\sin\left[(k-l)\Delta\phi\right]}{(k-l)\pi} e^{i(k-l)x} & \text{if} \quad k\neq l, \end{cases} \tag{D5}$$

such that

$$\begin{aligned} \frac{1}{2\pi}\int_{x-\Delta\phi}^{x+\Delta\phi} d\phi |n\rangle\langle n|_{\theta,\phi} = &\sum_{k=0}^{n}\binom{n}{k}\frac{\Delta\phi}{\pi}\cos^{2(n-k)}\left(\frac{\theta}{2}\right)\sin^{2k}\left(\frac{\theta}{2}\right)|n-k,k\rangle\langle n-k,k| \\ &+\sum_{k=1}^{n}\sum_{l<k}\sqrt{\binom{n}{k}\binom{n}{l}}\frac{\sin\left[(k-l)\Delta\phi\right]}{(k-l)\pi}\cos^{2n-(k+l)}\left(\frac{\theta}{2}\right)\sin^{k+l}\left(\frac{\theta}{2}\right) \\ &\times\left[e^{i(k-l)x}|n-k,k\rangle\langle n-l,l|+e^{-i(k-l)x}|n-l,l\rangle\langle n-k,k|\right]. \end{aligned} \tag{D6}$$

Note that this result is obtained by simply splitting $|n\rangle\langle n|_{\theta,\phi}$ in equation (D3) into diagonal and off-diagonal terms (in the $\mathcal{B}_n$ basis), and then using equation (D5) for the integration in ϕ. Finally, plugging equation (D6) into equation (D4) yields

$$\begin{aligned} \tilde{\sigma}_{x,j,n} = &\sum_{k=0}^{n}\binom{n}{k}\frac{\Delta\phi}{\pi}\left\{\int_{\frac{\pi}{2}-\Delta\theta}^{\frac{\pi}{2}+\Delta\theta}\mathrm{d}\theta\cos^{2(n-k)}\left(\frac{\theta}{2}\right)\sin^{2k}\left(\frac{\theta}{2}\right)\int_{I_j}\mathrm{d}I f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I)\frac{e^{-I}I^n}{n!}\right\}\times|n-k,k\rangle\langle n-k,k| \\ &+\sum_{k=1}^{n}\sum_{l<k}\sqrt{\binom{n}{k}\binom{n}{l}}\frac{\sin\left[(k-l)\Delta\phi\right]}{(k-l)\pi}\left\{\int_{\frac{\pi}{2}-\Delta\theta}^{\frac{\pi}{2}+\Delta\theta}\mathrm{d}\theta\cos^{2n-(k+l)}\left(\frac{\theta}{2}\right)\sin^{k+l}\left(\frac{\theta}{2}\right)\int_{I_j}\mathrm{d}I f_{\boldsymbol{\theta},\boldsymbol{I}}(\theta,I)\frac{e^{-I}I^n}{n!}\right\} \\ &\times\left[e^{i(k-l)x}|n-k,k\rangle\langle n-l,l|+e^{-i(k-l)x}|n-l,l\rangle\langle n-k,k|\right]. \end{aligned} \tag{D7}$$

Now, we make use of the canonical isomorphism:

$$|n,0\rangle\to[1\,0\ldots0]^t,\ |n-1,1\rangle\to[0\,1\ldots0]^t,\ \ldots\ ,\ |0,n\rangle\to[0\ldots0\,1]^t. \tag{D8}$$

This provides a natural matrix representation of the $\sigma_{x,j,n}$, where the (r,s)th entry is given by

$$\langle n-r+1,r-1|\,\sigma_{x,j,n}\,|n-s+1,s-1\rangle \tag{D9}$$

for $r,s=1,\ldots,n+1$. These matrices can be written down in any scientific computing tool for the numerical calculation of the TD via the eigenvalues, as indicated in appendix C.

Appendix E. Derivation of equation (32)

The goal is to show that

$$\frac{1}{\sqrt{2}}\left(|0\rangle_{\mathrm{A}'}|\Psi_{0,s,1}\rangle_{\mathrm{AB}}+|\pi\rangle_{\mathrm{A}'}|\Psi_{\pi,s,1}\rangle_{\mathrm{AB}}\right)=\frac{1}{\sqrt{2}}\left(\left|\frac{\pi}{2}\right\rangle_{\mathrm{A}'}\left|\Psi_{-\frac{\pi}{2},s,1}\right\rangle_{\mathrm{AB}}+\left|-\frac{\pi}{2}\right\rangle_{\mathrm{A}'}\left|\Psi_{\frac{\pi}{2},s,1}\right\rangle_{\mathrm{AB}}\right). \tag{E1}$$

From the RL Bloch sphere notation, $|y\rangle_{\mathrm{A}'}=\frac{1}{\sqrt{2}}\left(|\mathrm{R}\rangle_{\mathrm{A}'}+e^{iy}|\mathrm{L}\rangle_{\mathrm{A}'}\right)$, one can readily show that

$$|0\rangle_{\mathrm{A}'}=\frac{e^{-i\frac{\pi}{4}}}{\sqrt{2}}\left(\left|\frac{\pi}{2}\right\rangle_{\mathrm{A}'}+i\left|-\frac{\pi}{2}\right\rangle_{\mathrm{A}'}\right)\ \text{and}\ |\pi\rangle_{\mathrm{A}'}=\frac{e^{i\frac{\pi}{4}}}{\sqrt{2}}\left(\left|\frac{\pi}{2}\right\rangle_{\mathrm{A}'}-i\left|-\frac{\pi}{2}\right\rangle_{\mathrm{A}'}\right), \tag{E2}$$

where we keep the global phases for clarity. Plugging these relations into the l.h.s. of equation (E1) and reordering yields

$$\begin{aligned} &\frac{1}{\sqrt{2}}\left(|0\rangle_{\mathrm{A}'}|\Psi_{0,s,1}\rangle_{\mathrm{AB}}+|\pi\rangle_{\mathrm{A}'}|\Psi_{\pi,s,1}\rangle_{\mathrm{AB}}\right) \\ &=\frac{1}{\sqrt{2}}\left(\left|\frac{\pi}{2}\right\rangle_{\mathrm{A}'}\frac{e^{-i\frac{\pi}{4}}|\Psi_{0,s,1}\rangle_{\mathrm{AB}}+e^{i\frac{\pi}{4}}|\Psi_{\pi,s,1}\rangle_{\mathrm{AB}}}{\sqrt{2}}+\left|-\frac{\pi}{2}\right\rangle_{\mathrm{A}'}\frac{e^{i\frac{\pi}{4}}|\Psi_{0,s,1}\rangle_{\mathrm{AB}}+e^{-i\frac{\pi}{4}}|\Psi_{\pi,s,1}\rangle_{\mathrm{AB}}}{\sqrt{2}}\right). \end{aligned} \tag{E3}$$

Similarly, from the definition of $|\Psi_{x,s,1}\rangle_{AB}$ (given in equation (30)) and the RL Bloch sphere notation for system B, $|x\rangle_B = \frac{1}{\sqrt{2}}\left(|R\rangle_B + e^{ix}|L\rangle_B\right)$, one can easily show that

$$\frac{e^{-i\frac{\pi}{4}}|\Psi_{0,s,1}\rangle_{AB} + e^{i\frac{\pi}{4}}|\Psi_{\pi,s,1}\rangle_{AB}}{\sqrt{2}} = \left|\Psi_{-\frac{\pi}{2},s,1}\right\rangle_{AB} \text{ and } \frac{e^{i\frac{\pi}{4}}|\Psi_{0,s,1}\rangle_{AB} + e^{-i\frac{\pi}{4}}|\Psi_{\pi,s,1}\rangle_{AB}}{\sqrt{2}} = \left|\Psi_{\frac{\pi}{2},s,1}\right\rangle_{AB}. \quad \text{(E4)}$$

Plugging these relations into equation (E3), equation (E1) follows.

Appendix F. Channel model

Here, we present the channel model that we use for the simulations. As shown in section 2, the PT generates the phase-randomized WCP

$$\rho_w^{I,\theta,\phi} = \sum_{n=0}^{\infty} \frac{e^{-I}I^n}{n!}|n\rangle\langle n|_{\theta,\phi} \quad \text{(F1)}$$

in, say spatial mode w, with a known probability density function $f_{\phi,\theta,I}$. This state can also be written in the form

$$\rho_w^{I,\theta,\phi} = \frac{1}{2\pi}\int_0^{2\pi} d\psi |\sqrt{I}\,e^{i\psi}\rangle\langle\sqrt{I}\,e^{i\psi}|_{w,\theta,\phi}, \quad \text{(F2)}$$

such that one can apply the channel model to the pure state $\left|\sqrt{I}\,e^{i\psi}\right\rangle_{w,\theta,\phi}$ first and proceed with the phase-averaging later on. This is what we do next. The process that $\left|\sqrt{I}\,e^{i\psi}\right\rangle_{w,\theta,\phi}$ undergoes is illustrated in figure 5.

The BS transformation simply maps $\left|\sqrt{I}\,e^{i\psi}\right\rangle_{w,\theta,\phi}$ (in spatial mode w in the figure) to $\left|\sqrt{I\eta}\,e^{i\psi}\right\rangle_{a,\theta,\phi}$ (in spatial mode a in the figure). Now, in order to describe the measurement statistics of the basis-matched events, it suffices to contemplate one basis. For instance, let us consider that the generated state $\left|\sqrt{I}\,e^{i\psi}\right\rangle_{w,\theta,\phi}$ lies in the Z basis acceptance region —meaning that $(\phi,\theta,I) \in \Omega_j^Z$ for some $j \in \{s,d,v\}$— and Bob selects the Z basis for his measurement too —meaning that the polarization rotator does not alter the incident polarization—. Aiming to incorporate the action of the PBS, we recall that $\left|\sqrt{I\eta}\,e^{i\psi}\right\rangle_{a,\theta,\phi} = \exp\left\{\sqrt{I\eta}e^{i\psi}a_{\theta,\phi}^\dagger - \sqrt{I\eta}e^{-i\psi}a_{\theta,\phi}\right\}|vac\rangle$ with $a_{\theta,\phi}^\dagger = \cos(\theta/2)\,a_R^\dagger + e^{i\phi}\sin(\theta/2)\,a_L^\dagger$, and rewrite this state in terms of the creation operators associated to the Z basis, defined as $a_H^\dagger = a_{\frac{\pi}{2},0}^\dagger$, $a_V^\dagger = a_{\frac{\pi}{2},\pi}^\dagger$. This yields

$$\begin{aligned}\left|\sqrt{I\eta}\,e^{i\psi}\right\rangle_{a,\theta,\phi} = \exp\Bigg\{\sqrt{\frac{I\eta}{2}}e^{i\psi}\Big[\Big(\cos(\theta/2) + e^{i\phi}\sin(\theta/2)\Big)a_H^\dagger \\ + \Big(\cos(\theta/2) - e^{i\phi}\sin(\theta/2)\Big)a_V^\dagger\Big] - \widehat{\text{h.c.}}\Bigg\}|vac\rangle.\end{aligned} \quad \text{(F3)}$$

The transformation of the PBS reads $\left\{a_H^\dagger \to b_H^\dagger,\ a_V^\dagger \to c_V^\dagger\right\}$, which maps $\left|\sqrt{I\eta}\,e^{i\psi}\right\rangle_{a,\theta,\phi}$ to

$$\begin{aligned}&\left|\sqrt{\frac{I\eta}{2}}e^{i\psi}\Big(\cos(\theta/2) + e^{i\phi}\sin(\theta/2)\Big)\right\rangle_{b,\frac{\pi}{2},0}\left|\sqrt{\frac{I\eta}{2}}e^{i\psi}\Big(\cos(\theta/2) - e^{i\phi}\sin(\theta/2)\Big)\right\rangle_{c,\frac{\pi}{2},\pi} \\ &= \left|\sqrt{\frac{I\eta(1+\sin\theta\cos\phi)}{2}}e^{i\Gamma_+}\right\rangle_{b,\frac{\pi}{2},0}\left|\sqrt{\frac{I\eta(1-\sin\theta\cos\phi)}{2}}e^{i\Gamma_-}\right\rangle_{c,\frac{\pi}{2},\pi},\end{aligned} \quad \text{(F4)}$$

for known phases Γ_+ and Γ_- irrelevant to the discussion.

Coming next, the measurement implemented by each photo-detector is described by a POVM with elements $\{\hat{E}_{\text{no click}} = (1-p_d)|0\rangle\langle 0|, \hat{E}_{\text{click}} = \mathbb{1} - \hat{E}_{\text{no click}}\}$, where p_d stands for the dark count probability and $\mathbb{1}$ stands for the identity operator (note that detector loss has already been accounted for in the channel). Denoting the first (second) ket in the r.h.s. of equation (F4) by $|B\rangle$ ($|C\rangle$), it follows that detectors 'H' and 'V' in figure 5 record a click with independent probabilities $p_H = \text{Tr}\left[\hat{E}_{\text{click}}|B\rangle\langle B|\right]$ and $p_V = \text{Tr}\left[\hat{E}_{\text{click}}|C\rangle\langle C|\right]$, such that

$$p_H = 1 - (1-p_d)e^{-\frac{I\eta(1+\sin\theta\cos\phi)}{2}} \quad \text{and} \quad p_V = 1 - (1-p_d)e^{-\frac{I\eta(1-\sin\theta\cos\phi)}{2}}. \quad \text{(F5)}$$

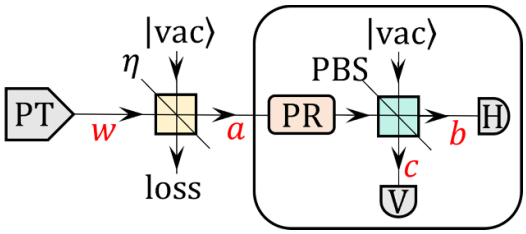

Figure 5. Schematic of the channel model. The quantum states generated in the PT undergo (1) a lossy quantum channel and (2) a quantum measurement at Bob's lab. The measurement is modelled with a polarization rotator (PR) that selects Bob's basis setting, followed by a PBS that splits orthogonal polarizations in the Z basis (say, H and (V). A noisy-and-lossy threshold detector is located in each output port of the PBS and we assume that both detectors are equal. Notably, channel and detector loss are jointly accounted for with a BS of effective transmittance $\eta = \eta_{\rm ch}\eta_{\rm det}$, where $\eta_{\rm ch}$ ($\eta_{\rm det}$) stands for the channel transmittance (detection efficiency). Also, the relevant spatial modes are indicated in red.

These probabilities do not depend on the phase ψ, which implies that they remain unchanged after phase averaging. In short, $\rho_w^{I,\theta,\phi}$ triggers a click when measured in the Z basis with overall probability

$$p\left(\text{click}\middle|\rho_w^{I,\theta,\phi},Z\right) = 1 - p\left(\text{no click}\middle|\rho_w^{I,\theta,\phi},Z\right) = 1-(1-p_{\rm H})(1-p_{\rm V}) = 1-(1-p_{\rm d})^2 e^{-I\eta}. \tag{F6}$$

Notably, equation (F6) does not use the fact that $\rho_w^{I,\theta,\phi}$ belongs to a Z basis acceptance region in any way. This consideration only matters for the calculation of the error probability $p\left(\text{err}\middle|\rho_w^{I,\theta,\phi},Z\right)$, which we do next. For this purpose, we further assume that $\rho_w^{I,\theta,\phi}$ belongs to an acceptance region associated to the horizontal polarization. This amounts to saying that $\phi \in [x-\Delta\phi, x+\Delta\phi]$ with $x=0$, or equivalently that $(\phi,\theta,I) \in \Omega_{0,j}$ for some $j \in \{\text{s},\text{d},\text{v}\}$. In this case, a bit error occurs if the outcome 'V' is recorded. Considering, as usual, that double-clicks are randomly assigned to a specific outcome, this means that $p\left(\text{err}\middle|\rho_w^{I,\theta,\phi},Z\right) = p_{\rm V}(1-p_{\rm H}) + p_{\rm V}p_{\rm H}/2$ for all $(\phi,\theta,I) \in \Omega_{0,j}$, which is easily taken to the form

$$p\left(\text{err}\middle|\rho_w^{I,\theta,\phi},Z\right) = \frac{1}{2}\left[1-(1-p_{\rm d})^2 e^{-I\eta}\right] - \frac{1}{2}(1-p_{\rm d})\left[e^{-\frac{I\eta(1-\sin\theta\cos\phi)}{2}} - e^{-\frac{I\eta(1+\sin\theta\cos\phi)}{2}}\right]. \tag{F7}$$

Finally, given equations (F6) and (F7), it is straightforward to compute $Q_j^Z = p\left(\text{click}\middle|\sigma_j^Z,Z\right)$ and $E_j^Z = p\left(\text{err}\middle|\sigma_j^Z,Z\right)$. To be precise, since $\sigma_j^Z = \left\langle\rho_w^{I,\theta,\phi}\right\rangle_{\Omega_j^Z}/\langle 1\rangle_{\Omega_j^Z}$, it follows that

$$Q_j^Z = \frac{\left\langle p\left(\text{click}\middle|\rho_w^{I,\theta,\phi},Z\right)\right\rangle_{\Omega_j^Z}}{\langle 1\rangle_{\Omega_j^Z}} = 1-(1-p_{\rm d})^2\frac{\left\langle e^{-I\eta}\right\rangle_{\Omega_j^Z}}{\langle 1\rangle_{\Omega_j^Z}}. \tag{F8}$$

On the other hand, $E_j^Z = \left(p\left(\text{err}\middle|\sigma_{0,j},Z\right) + p\left(\text{err}\middle|\sigma_{\pi,j},Z\right)\right)/2$, and both $\sigma_{0,j}$ and $\sigma_{\pi,j}$ are equally likely to trigger an error for symmetry reasons within our channel model. Therefore, $E_j^Z = p\left(\text{err}\middle|\sigma_{0,j},Z\right)$, and thus

$$E_j^Z = \frac{\left\langle p\left(\text{err}\middle|\rho_w^{I,\theta,\phi},Z\right)\right\rangle_{\Omega_{0,j}}}{\langle 1\rangle_{\Omega_{0,j}}} = \frac{1}{2}\left[1-(1-p_{\rm d})^2\frac{\left\langle e^{-I\eta}\right\rangle_{\Omega_{0,j}}}{\langle 1\rangle_{\Omega_{0,j}}}\right]$$
$$-\frac{1}{2}(1-p_{\rm d})\left[\frac{\left\langle e^{-\frac{I\eta(1-\sin\theta\cos\phi)}{2}}\right\rangle_{\Omega_{0,j}}}{\langle 1\rangle_{\Omega_{0,j}}} - \frac{\left\langle e^{-\frac{I\eta(1+\sin\theta\cos\phi)}{2}}\right\rangle_{\Omega_{0,j}}}{\langle 1\rangle_{\Omega_{0,j}}}\right]. \tag{F9}$$

ORCID iDs

Víctor Zapatero https://orcid.org/0000-0002-0951-8450
Marcos Curty https://orcid.org/0000-0002-0330-6828

References

[1] Portmann C and Renner R 2022 Security in quantum cryptography *Rev. Mod. Phys.* **94** 025008
[2] Lo H-K, Curty M and Tamaki K 2014 Secure quantum key distribution *Nat. Photon.* **8** 595
[3] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002
[4] Vakhitov A, Makarov V and Hjelme D R 2001 Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography *J. Mod. Opt.* **48** 2023–38
[5] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 Trojan-horse attacks on quantum-key-distribution systems *Phys. Rev.* A **73** 022320
[6] Jain N, Stiller B, Khan I, Makarov V, Marquardt C and Leuchs G 2014 Risk analysis of Trojan-horse attacks on practical quantum key distribution systems *IEEE J. Sel. Top. Quantum Electron.* **21** 168–77
[7] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C and Leuchs G 2014 Trojan-horse attacks threaten the security of practical quantum cryptography *New J. Phys.* **16** 123030
[8] Sajeed S, Minshull C, Jain N and Makarov V 2017 Invisible Trojan-horse attack *Sci. Rep.* **7** 1–7
[9] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z L and Shields A J 2015 Practical security bounds against the Trojan-horse attack in quantum key distribution *Phys. Rev.* X **5** 031030
[10] Tamaki K, Curty M and Lucamarini M 2016 Decoy-state quantum key distribution with a leaky source *New J. Phys.* **18** 065008
[11] Wang W, Tamaki K and Curty M 2018 Finite-key security analysis for quantum key distribution with leaky sources *New J. Phys.* **20** 083027
[12] Navarrete A and Curty M 2022 Improved finite-key security analysis of quantum key distribution against Trojan-horse attacks *Quantum Sci. Technol.* **7** 035021
[13] Liu B *et al* 2021 Fully passive entanglement based quantum key distribution scheme (arXiv:2111.03211)
[14] Paraïso T K *et al* 2019 A modulator-free quantum key distribution transmitter chip *npj Quantum Inf.* **5** 1–6
[15] Mauerer W and Silberhorn C 2007 Quantum key distribution with passive decoy state selection *Phys. Rev.* A **75** 050305
[16] Wang Q, Wang X-B, Björk G and Karlsson A 2007 Improved practical decoy state method in quantum key distribution with parametric down-conversion source *Europhys. Lett.* **79** 40001
[17] Adachi Y, Yamamoto T, Koashi M and Imoto N 2007 Simple and efficient quantum key distribution with parametric down-conversion *Phys. Rev. Lett.* **99** 180503
[18] Ma X and Lo H-K 2008 Quantum key distribution with triggering parametric down-conversion sources *New J. Phys.* **10** 073018
[19] Adachi Y, Yamamoto T, Koashi M and Imoto N 2009 Boosting up quantum key distribution by learning statistics of practical single-photon sources *New J. Phys.* **11** 113033
[20] Wang Q, Zhang C-H and Wang X-B 2016 Scheme for realizing passive quantum key distribution with heralded single-photon sources *Phys. Rev.* A **93** 032312
[21] Curty M, Moroder T, Ma X and Lütkenhaus N 2009 Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution *Opt. Lett.* **34** 3238–40
[22] Curty M, Ma X, Qi B and Moroder T 2010 Passive decoy-state quantum key distribution with practical light sources *Phys. Rev.* A **81** 022310
[23] Li Y, Bao W-S, Li H-W, Zhou C and Wang Y 2014 Passive decoy-state quantum key distribution using weak coherent pulses with intensity fluctuations *Phys. Rev.* A **89** 032329
[24] Shan Y-Z, Sun S-H, Ma X-C, Jiang M-S, Zhou Y-L and Liang L-M 2014 Measurement-device-independent quantum key distribution with a passive decoy-state method *Phys. Rev.* A **90** 042334
[25] Zhang Y *et al* 2010 Practical non-Poissonian light source for passive decoy state quantum key distribution *Opt. Lett.* **35** 3393–5
[26] Zhang Y *et al* 2012 Experimental demonstration of passive decoy state quantum key distribution *Chin. Phys.* B **21** 100307
[27] Krapick S, Stefszky M S, Jachura M, Brecht B, Avenhaus M and Silberhorn C 2014 Bright integrated photon-pair source for practical passive decoy-state quantum key distribution *Phys. Rev.* A **89** 012329
[28] Sun Q-C *et al* 2014 Experimental passive decoy-state quantum key distribution *Laser Phys. Lett.* **11** 085202
[29] Guan J-Y *et al* 2015 Experimental passive round-Robin differential phase-shift quantum key distribution *Phys. Rev. Lett.* **114** 180502
[30] Sun S-H, Tang G-Z, Li C-Y and Liang L-M 2016 Experimental demonstration of passive-decoy-state quantum key distribution with two independent lasers *Phys. Rev.* A **94** 032324
[31] Curty M, Ma X, Lo H-K and Lütkenhaus N 2010 Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals *Phys. Rev.* A **82** 052325
[32] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems & Signal Processing* (Bangalore: IEEE) pp 175–9
[33] Curty M, Jofre M, Pruneri V and Mitchell M W 2015 Passive decoy-state quantum key distribution with coherent light *Entropy* **17** 4064–82
[34] Boyd R W 2008 *Nonlinear Optics* (Waltham, MA: Academic)
[35] Wang W *et al* 2022 Fully-passive quantum key distribution (arXiv:2207.05916)
[36] Nielsen M and Chuang I 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[37] Renner R 2007 Symmetry of large physical systems implies independence of subsystems *Nat. Phys.* **3** 645–9
[38] Christandl M, König R and Renner R 2009 Postselection technique for quantum channels with applications to quantum cryptography *Phys. Rev. Lett.* **102** 020504
[39] Tomamichel M and Renner R 2011 Uncertainty relation for smooth entropies *Phys. Rev. Lett.* **106** 110506
[40] Sun S-H, Gao M, Jiang M-S, Li C-Y and Liang L-M 2012 Partially random phase attack to the practical two-way quantum-key-distribution system *Phys. Rev.* A **85** 032304
[41] Sun S-H, Xu F, Jiang M-S, Ma X-C, Lo H-K and Liang L-M 2015 Effect of source tampering in the security of quantum cryptography *Phys. Rev.* A **92** 022304

[42] Huang A, Navarrete A, Sun S-H, Chaiwongkhot P, Curty M and Makarov V 2019 Laser-seeding attack in quantum key distribution *Phys. Rev. Appl.* **12** 064043
[43] Huang A, Li R, Egorov V, Tchouragoulov S, Kumar K and Makarov V 2020 Laser-damage attack against optical attenuators in quantum key distribution *Phys. Rev. Appl.* **13** 034017
[44] Zhang G, Primaatmaja I W, Haw J Y, Gong X, Wang C and Lim C C W 2021 Securing practical quantum communication systems with optical power limiters *PRX Quantum* **2** 030304
[45] Ponosova A, Ruzhitskaya D, Chaiwongkhot P, Egorov V, Makarov V and Huang A 2022 Protecting fiber-optic quantum key distribution sources against light-injection attacks *PRX Quantum* **3** 040307