Finite-key security of passive quantum key distribution

Víctor Zapatero[1,2,3,*] 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*

(Received 7 August 2023; revised 5 December 2023; accepted 22 December 2023; published 11 January 2024)

The passive approach to quantum key distribution (QKD) eliminates all optical modulators and random number generators from QKD systems reaching an enhanced simplicity, immunity to modulator side channels, and potentially higher repetition rates. In this work, we provide finite-key security bounds for a fully passive decoy-state Bennett-Brassard 1984 (BB84) protocol, considering a recently presented passive QKD source. With our analysis, the attainable secret-key rate is comparable to that of the perfect parameter-estimation limit, in fact differing from the key rate of the active approach by less than one order of magnitude. This demonstrates the practicality of fully passive QKD solutions.

DOI: 10.1103/PhysRevApplied.21.014018

I. INTRODUCTION

Quantum key distribution (QKD) allows one to establish information-theoretically secure keys between remote locations through an insecure channel [1]. This security standard, which is a must to achieve long-term security guarantees, makes QKD a unique solution for private communications with the highest requisites. Since its conception in 1984 [2], QKD has experienced remarkable progress. Nowadays, specialized companies supply integral QKD services [3–6], metropolitan QKD networks are being installed around the globe [7–10], and a space-ground integrated QKD backbone with an extension of thousands of kilometers has been deployed [11].

Notably though, QKD security proofs rely on mathematical models that describe the behavior of the QKD equipment, in so doing, opening the door for mischaracterization loopholes. For this reason, strictly quantifying the level of security of QKD implementations is a thorny issue [12] and a critical vulnerability of real-life QKD systems is active modulation. Indeed, active modulators can be a source of information leakage in different ways; e.g., negligently encoding private information in undesired degrees of freedom, introducing correlations between adjacent pulses [13–15], or serving as a target for Trojan-horse attacks (THAs) [16–20]. In the latter case, an eavesdropper (Eve) injects bright light pulses into a QKD system and measures the back-reflected light, possibly extracting information about the setting choices. In particular, since the back-reflected light has passed through the modulators, it may be encoded with the same information as the signals prepared by the sender (Alice) or it may reveal the measurement basis selected by the receiver (Bob). In this regard, although one can model the information leakage and account for it in the estimation of the secret-key length, this approach may severely affect the achievable performance of QKD according to the existing analyses [21–24], unless sufficiently strong isolation is introduced. From this perspective, a better solution is provided by passive QKD, which eliminates all active modulation from QKD devices and replaces it by postselection. Remarkably, this solution not only confers immunity to modulator side channels but it may also simplify the hardware layout and boost the clock rate of a QKD system, at the price of (i) reducing the secret-key rate per pulse by roughly an order of magnitude and (ii) incorporating a measurement unit at Alice's source for the postselection of the desired states. Naturally, this unit must be well characterized and properly isolated and a detailed security evaluation of the possible security loopholes that may arise from it is essential in practice.

As an example, one can use coherent light to passively generate decoy states in different ways [25–28] (see also the experimental reports in Refs. [29–33]) or to passively prepare random photon polarizations in a plane for a passive realization of the Bennett-Brassard 1984 (BB84) protocol [34]. Notably as well, passive BB84 encoding and passive decoy-state preparation can be combined in a single linear optical setup, as recently shown in Refs. [35,36]. Indeed, these two papers were soon followed by pioneering experiments that prove the feasibility of fully passive QKD [37,38] and, in fact, fully passive twin-field QKD has also been envisioned [39]. What is more, the passive approach

[*] vzapatero@vqcc.uvigo.es

may be of practical benefit in quantum cryptographic primitives other than QKD [40–42].

Considering the passive source devised in Ref. [36], in this work we present finite-key security bounds against sequential attacks for a fully passive decoy-state BB84 protocol, carefully merging the encoding strategy of Ref. [35] with a sophistication of the parameter-estimation method in Ref. [36]. Remarkably, the secret-key rate per pulse attainable with our analysis and our passive scheme is closer than previously reported to the corresponding key rate with an active setup.

The structure of the paper is as follows. In Sec. II, we list the assumptions that underlie our security analysis. In Sec. III, we provide a characterization of the passive QKD source that we consider. In Sec. IV, we describe the encoding scheme that we adopt, together with an insightful entanglement-based picture that arises from it. In Sec. V, we give a description of the passive decoy-state BB84 protocol that we contemplate. Section VI contains all the details of the decoy-state method and in Sec. VII we derive the necessary estimates for the secret-key parameters. Finally, in Sec. VIII we illustrate the performance of the proposed analysis and in Sec. IX we present a series of concluding remarks. For the reproducibility of the results, various appendices are included at the end of the paper as well.

II. ASSUMPTIONS

Let us start by enumerating the various assumptions on which our analysis relies.

A. Assumptions on Alice's and Bob's devices

For the characterization of the fully passive source, we assume: (i) perfect phase randomization and intensity control of the prepared coherent pulses, (ii) perfect-visibility interference at the beam splitters and polarizing beam splitters (thus requiring perfect control of the frequency, time, and polarization modes), (iii) noiseless polarization and intensity measurements in Alice's measurement unit (enabling the accurate determination of these quantities), (iv) no information leakage from Alice's measurement unit, and (v) no influence of Eve on the outcomes of Alice's measurement unit. Importantly, assumptions (iv) and (v) might require careful shielding of the classical photodiodes. As for Bob's measurement unit, we adopt the standard basis-independent detection-efficiency assumption. Note, however, that this latter assumption could be removed by considering a measurement-device-independent configuration [43].

B. Sequentiality assumption

We assume that Eve holds a quantum probe, E, and a classical register, R, and consider the following round-by-round model. In the first round, she initializes her probe E to an arbitrary state, $\xi_{\mathrm{E}}^{(1)}$, and couples it to the signal in the channel through an arbitrary unitary operation, $\hat{U}_{\mathrm{BE}}^{(1)}$. At the end of the round, based on $\hat{U}_{\mathrm{BE}}^{(1)}$, $\xi_{\mathrm{E}}^{(1)}$ and the outcome of a potential measurement on E, the classical register R updates from an initial state R_0 to a new state R_1, which determines (i) Eve's choice for the next unitary operation, $\hat{U}_{\mathrm{BE}}^{(2)}$, and (ii) how the state of the probe system E is updated to a new state $\xi_{\mathrm{E}}^{(2)}$. Subsequent rounds proceed in the same way: at the end of round u, the state of the register, R_u, fully determines Eve's next intervention, which is generally influenced by the record of all unitaries, $\{\hat{U}_{\mathrm{BE}}^{(v)}\}_{v\leq u}$, probe states, $\{\xi_{\mathrm{E}}^{(v)}\}_{v\leq u}$, and measurement outcomes.

Importantly, a consequence of this model is that earlier rounds can only affect the uth round through their influence on R_{u-1}. From a technical point of view, the model is invoked to assure that the trace-distance (TD) argument of Appendix A is applicable to the conditional detection statistics of Kato's inequality [44]. As an example, a similar adversary model is required in finite-key analyses based on the reference technique [13] (see, e.g., Ref. [24]) or in order to apply the generalized entropy-accumulation theorem [45] to device-dependent protocols [46]. This said, we remark that if each protocol round starts only after the conclusion of the previous one—a sequential structure that can be practically enforced by Alice and Bob—this adversary model is fully general.

III. CHARACTERIZATION OF THE FULLY PASSIVE SOURCE

The passive source that we consider is due to Ref. [36] and is shown in Fig. 1. Although it uses four independent lasers, it can also be realized with an equivalent single-laser configuration and suitable interferometry, as discussed in Refs. [35,36] and implemented in Refs. [37,38].

In the figure, $|\tau\rangle_{\mathrm{R(L)}}$ denotes a right-handed (left-handed) circularly polarized coherent state with complex amplitude $\tau \in \mathbb{C}$. That is to say, $|\tau\rangle_{\mathrm{R(L)}} = \exp\{\tau a_{\mathrm{R(L)}}^{\dagger} - \tau^{*} a_{\mathrm{R(L)}}\} |\mathrm{vac}\rangle$, where $|\mathrm{vac}\rangle$ is the vacuum state and $a_{\mathrm{R(L)}}^{\dagger}$ and $a_{\mathrm{R(L)}}$, respectively, denote the creation and annihilation operators of a right-handed (left-handed) circular-polarization mode. Throughout this work, we shall refer to the Bloch sphere spanned by $|\mathrm{R}\rangle = a_{\mathrm{R}}^{\dagger} |\mathrm{vac}\rangle$ and $|\mathrm{L}\rangle = a_{\mathrm{L}}^{\dagger} |\mathrm{vac}\rangle$ as the RL sphere, an arbitrary state of which reads

$$\cos\left(\frac{\theta}{2}\right) |\mathrm{R}\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right) |\mathrm{L}\rangle , \qquad (1)$$

for $\theta \in [0, \pi]$ (polar angle) and $\phi \in (-\pi, \pi]$ (azimuthal angle). As shown in Ref. [36], the mixed output state of

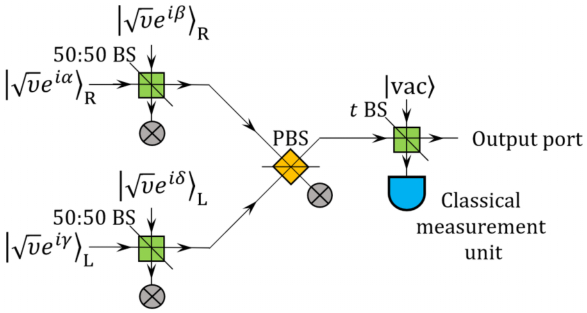
$|\sqrt{v}e^{i\beta}\rangle_{\mathrm{R}}$
50:50 BS
$|\sqrt{v}e^{i\alpha}\rangle_{\mathrm{R}}$
$|\mathrm{vac}\rangle$
t BS
PBS
Output port
$|\sqrt{v}e^{i\delta}\rangle_{\mathrm{L}}$
50:50 BS
$|\sqrt{v}e^{i\gamma}\rangle_{\mathrm{L}}$
Classical measurement unit

FIG. 1. The possible architecture of a fully passive QKD source due to Ref. [36]. All coherent states in the figure have a common large intensity ν and independent random phases α, β, γ, and δ. These random phases can be achieved by operating the lasers under gain-switching conditions, i.e., by turning the lasers on and off between pulses. The interference in the 50:50 beam splitter (BS) of the top (bottom) arm yields a coherent state with random intensity [26]—dependent on the phase difference $\beta - \alpha$ ($\delta - \gamma$)—and right-handed (left-handed) circular polarization, R (L). When these two pulses interfere in the polarizing BS (PBS), a new coherent state is generated, the intensity of which is the sum of the input intensities and the polarization of which is randomly distributed in the RL sphere defined in the main text. Lastly, this final state enters a BS with transmittance $t \ll 1$. The transmitted signal, which is attenuated to the single-photon level, is sent to Bob and the reflected signal reaches a classical measurement unit for the accurate determination of the prepared intensity and polarization. Unused spatial modes are tagged by the symbol "⊗" in the figure.

the fully passive source reads

$$\sigma = \frac{1}{2\pi}\int_{-\pi}^{\pi} d\phi \int_{0}^{\pi} d\theta \int_{0}^{I_\theta^*} dI f\left(\theta, I\right) \sum_{n=0}^{\infty} \frac{e^{-I} I^n}{n!} \left|n\right\rangle \left\langle n\right|_{\theta,\phi}, \tag{2}$$

for

$$f\left(\theta, I\right) = \frac{1}{2\nu t \pi^2 \sqrt{1 - \frac{I}{2\nu t}\cos^2\left(\frac{\theta}{2}\right)}\sqrt{1 - \frac{I}{2\nu t}\sin^2\left(\frac{\theta}{2}\right)}},$$
$$\left|n\right\rangle_{\theta,\phi} = \frac{1}{n!}\left[\cos\left(\frac{\theta}{2}\right) a_{\mathrm{R}}^{\dagger} + e^{i\phi}\sin\left(\frac{\theta}{2}\right) a_{\mathrm{L}}^{\dagger}\right]^n \left|\mathrm{vac}\right\rangle, \tag{3}$$

and $I_\theta^* = \min\left\{2\nu t/\cos^2\left(\theta/2\right), 2\nu t/\sin^2\left(\theta/2\right)\right\}$, ν and t being introduced in Fig. 1. According to these equations, ϕ is uniformly distributed in the output state but θ is coupled to the intensity I.

IV. ENCODING SCHEME AND ENTANGLEMENT-BASED PICTURE

We select the encoding scheme of Ref. [35]—which postselects polar (equatorial) regions of the Bloch sphere for key generation (parameter estimation)—and the decoy-state scheme of Ref. [36]—which uses decoy intervals in both bases. According to our simulations, these choices lead to a better performance than, say, only postselecting equatorial regions for the encoding or using decoy states in the test basis alone.

To be precise, let Γ^{key} and Γ^{test} denote two arbitrary lists of settings. The postselection regions are given by

$$\Omega_j^{\mathrm{R}} = \left\{\phi \in (-\pi, \pi], \theta \in \left(0, \Delta\theta'\right), I \in I_j\right\},$$
$$\Omega_j^{\mathrm{L}} = \left\{\phi \in (-\pi, \pi], \theta \in \left(\pi - \Delta\theta', \pi\right), I \in I_j\right\} \tag{4}$$

with $j \in \Gamma^{\mathrm{key}}$ for key generation, and

$$\Omega_j^{\mathrm{H}} = \left\{\phi \in \left(-\Delta\phi, \Delta\phi\right), \theta \in \left(\frac{\pi}{2} - \Delta\theta, \frac{\pi}{2} + \Delta\theta\right), I \in I_j\right\},$$
$$\Omega_j^{\mathrm{V}} = \left\{\phi \in \left(\pi - \Delta\phi, \pi + \Delta\phi\right), \theta \in \left(\frac{\pi}{2} - \Delta\theta, \frac{\pi}{2} + \Delta\theta\right), I \in I_j\right\}, \tag{5}$$

with $j \in \Gamma^{\mathrm{test}}$ for parameter estimation (PE). The polarization acceptance regions in the RL sphere are illustrated in Fig. 2, where the notation $|\mathrm{H}\rangle = (|\mathrm{R}\rangle + |\mathrm{L}\rangle)/\sqrt{2}$ and $|\mathrm{V}\rangle = (|\mathrm{R}\rangle - |\mathrm{L}\rangle)/\sqrt{2}$ is introduced.

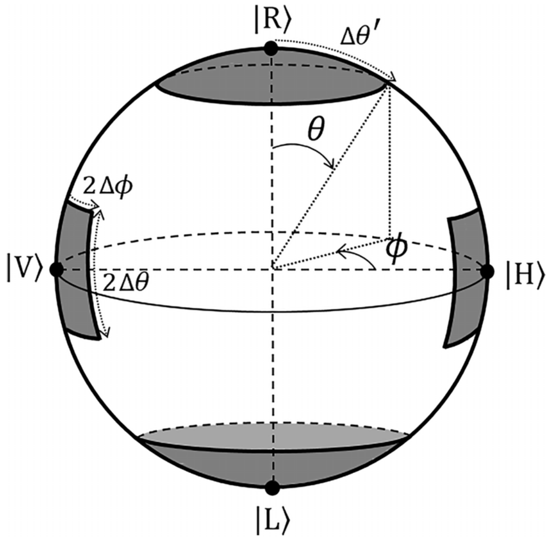

FIG. 2. Postselection of the encoding regions in the RL sphere. While $\Delta\theta'$ characterizes the key regions (polar caps), $\Delta\theta$ and $\Delta\phi$ characterize the test regions (rectangular stripes).

The postselected state that arises from the acceptance region $\Omega_j^{\mathrm{R(L)}}$ can be written as

$$\sigma_j^{\mathrm{R(L)}} = \frac{1}{\langle 1\rangle_{\Omega_j^{\mathrm{R(L)}}}} \left\langle \sum_{n=0}^{\infty} \frac{e^{-I} I^n}{n!} \left|n\right\rangle \left\langle n\right|_{\theta,\phi} \right\rangle_{\Omega_j^{\mathrm{R(L)}}}, \tag{6}$$

where $\langle\cdot\rangle_\Omega$ denotes averaging with the weight $f(\theta,I)/2\pi$ over the region Ω of the (ϕ,θ,I) space. Equation (6) trivially decomposes into a classical mixture of Fock states,

$$\sigma_j^{\mathrm{R(L)}} = \sum_{n=0}^{\infty} p_{n|j}^{\mathrm{key}} \sigma_{j,n}^{\mathrm{R(L)}}, \tag{7}$$

where we have introduced the shorthand notation $p_{n|j}^{\mathrm{key}} = \left\langle e^{-I} I^n/n! \right\rangle_{\Omega_j^{\mathrm{R}}} / \langle 1\rangle_{\Omega_j^{\mathrm{R}}} = \left\langle e^{-I} I^n/n! \right\rangle_{\Omega_j^{\mathrm{L}}} / \langle 1\rangle_{\Omega_j^{\mathrm{L}}}$ and $\sigma_{j,n}^{\mathrm{R(L)}} = \left\langle e^{-I} I^n/n! \left|n\right\rangle \left\langle n\right|_{\theta,\phi} \right\rangle_{\Omega_j^{\mathrm{R(L)}}} \big/ \left\langle e^{-I} I^n/n! \right\rangle_{\Omega_j^{\mathrm{R(L)}}}$. Naturally, the complete key-generation region of setting j, given by $\Omega_j^{\mathrm{key}} = \Omega_j^{\mathrm{R}} \cup \Omega_j^{\mathrm{L}}$, yields a state of the form $\sigma_j^{\mathrm{key}} = \sum_{n=0}^{\infty} p_{n|j}^{\mathrm{key}} \sigma_{j,n}^{\mathrm{key}}$, where

$$\sigma_{j,n}^{\mathrm{key}} = \frac{\sigma_{j,n}^{\mathrm{R}} + \sigma_{j,n}^{\mathrm{L}}}{2}. \tag{8}$$

As for the test regions, we define $\Omega_j^{\mathrm{test}} = \Omega_j^{\mathrm{H}} \cup \Omega_j^{\mathrm{V}}$ and denote the postselected states that arise from Ω_j^{H}, Ω_j^{V} and Ω_j^{test}, respectively, as σ_j^{H}, σ_j^{V} and σ_j^{test}, which satisfy relations that are completely analogous to those of Eqs. (6), (7), and (8). In particular, the test-basis Fock states read $\sigma_{j,n}^{\mathrm{H(V)}} = \left\langle e^{-I} I^n/n! \left|n\right\rangle \left\langle n\right|_{\theta,\phi} \right\rangle_{\Omega_j^{\mathrm{H(V)}}} \big/ \left\langle e^{-I} I^n/n! \right\rangle_{\Omega_j^{\mathrm{H(V)}}}$, and their corresponding photon-number statistics are $p_{n|j}^{\mathrm{test}} = \left\langle e^{-I} I^n/n! \right\rangle_{\Omega_j^{\mathrm{H}}} / \langle 1\rangle_{\Omega_j^{\mathrm{H}}} = \left\langle e^{-I} I^n/n! \right\rangle_{\Omega_j^{\mathrm{V}}} / \langle 1\rangle_{\Omega_j^{\mathrm{V}}}$.

Let us now focus on the single-photon components of σ_j^{R} and σ_j^{L}, from which the final key is ultimately extracted. Using the matrix representation of Appendix B, it follows that

$$\begin{aligned} \sigma_{j,1}^{\mathrm{R}} &= \frac{1+\lambda_j^{\mathrm{key}}}{2} \left|\mathrm{R}\right\rangle \left\langle \mathrm{R}\right| + \frac{1-\lambda_j^{\mathrm{key}}}{2} \left|\mathrm{L}\right\rangle \left\langle \mathrm{L}\right|, \\ \sigma_{j,1}^{\mathrm{L}} &= \frac{1+\lambda_j^{\mathrm{key}}}{2} \left|\mathrm{L}\right\rangle \left\langle \mathrm{L}\right| + \frac{1-\lambda_j^{\mathrm{key}}}{2} \left|\mathrm{R}\right\rangle \left\langle \mathrm{R}\right|, \end{aligned} \tag{9}$$

for $\lambda_j^{\mathrm{key}} = \left\langle e^{-I} I \cos\theta \right\rangle_{\Omega_j^{\mathrm{R}}} \big/ \left\langle e^{-I} I \right\rangle_{\Omega_j^{\mathrm{R}}}$, meaning that the desired polarization is prepared with probability $(1+\lambda_j^{\mathrm{key}})/2$ and the orthogonal polarization is prepared otherwise. Without loss of generality, then, one can describe these states by considering a shield system S that stores the bit-flip information. This leads to the purified states

$$\begin{aligned} \left|\Psi_{j,1}^{\mathrm{R}}\right\rangle_{\mathrm{SB}} &= \sqrt{\frac{1+\lambda_j^{\mathrm{key}}}{2}} \left|0\right\rangle_{\mathrm{S}} \left|\mathrm{R}\right\rangle_{\mathrm{B}} + \sqrt{\frac{1-\lambda_j^{\mathrm{key}}}{2}} \left|1\right\rangle_{\mathrm{S}} \left|\mathrm{L}\right\rangle_{\mathrm{B}}, \\ \left|\Psi_{j,1}^{\mathrm{L}}\right\rangle_{\mathrm{SB}} &= \sqrt{\frac{1+\lambda_j^{\mathrm{key}}}{2}} \left|0\right\rangle_{\mathrm{S}} \left|\mathrm{L}\right\rangle_{\mathrm{B}} + \sqrt{\frac{1-\lambda_j^{\mathrm{key}}}{2}} \left|1\right\rangle_{\mathrm{S}} \left|\mathrm{R}\right\rangle_{\mathrm{B}}, \end{aligned} \tag{10}$$

where we have added the subscripts S and B for clarity (nonetheless, they will be omitted where possible). Further proceeding with the standard entanglement-based source-replacement scheme on Alice's side, with $\{\left|\mathrm{R}\right\rangle_{\mathrm{A}}, \left|\mathrm{L}\right\rangle_{\mathrm{A}}\}$ denoting an orthonormal basis of Alice's ancillary qubit A, we obtain the state

$$\left|\Psi_{j,1}\right\rangle_{\mathrm{ASB}} = \frac{1}{\sqrt{2}} \left(\left|\mathrm{R}\right\rangle_{\mathrm{A}} \left|\Psi_{j,1}^{\mathrm{R}}\right\rangle_{\mathrm{SB}} + \left|\mathrm{L}\right\rangle_{\mathrm{A}} \left|\Psi_{j,1}^{\mathrm{L}}\right\rangle_{\mathrm{SB}} \right), \tag{11}$$

which equivalently describes the state preparation every time a single photon is generated and Ω_j^{key} is postselected. Importantly, by introducing $\left|\mathrm{H}\right\rangle_{\mathrm{A}} = (\left|\mathrm{R}\right\rangle_{\mathrm{A}} + \left|\mathrm{L}\right\rangle_{\mathrm{A}})/\sqrt{2}$ and $\left|\mathrm{V}\right\rangle_{\mathrm{A}} = (\left|\mathrm{R}\right\rangle_{\mathrm{A}} - \left|\mathrm{L}\right\rangle_{\mathrm{A}})/\sqrt{2}$ and regrouping terms, $\left|\Psi_{j,1}\right\rangle_{\mathrm{ASB}}$ can be written as

$$\left|\Psi_{j,1}\right\rangle_{\mathrm{ASB}} = \frac{1}{\sqrt{2}} \left(\left|\mathrm{H}\right\rangle_{\mathrm{A}} \left|\beta_j^{+}\right\rangle_{\mathrm{S}} \left|\mathrm{H}\right\rangle_{\mathrm{B}} + \left|\mathrm{V}\right\rangle_{\mathrm{A}} \left|\beta_j^{-}\right\rangle_{\mathrm{S}} \left|\mathrm{V}\right\rangle_{\mathrm{B}} \right), \tag{12}$$

where the shield states are given by $\left|\beta_j^{\pm}\right\rangle_{\mathrm{S}} = [(1+\lambda_j^{\mathrm{key}})/2]^{1/2} \left|0\right\rangle_{\mathrm{S}} \pm \left[(1-\lambda_j^{\mathrm{key}})/2\right]^{1/2} \left|1\right\rangle_{\mathrm{S}}$.

In summary, if Alice measures her ancilla A of $\left|\Psi_{j,1}\right\rangle_{\mathrm{ASB}}$ in the key basis $\{\left|\mathrm{R}\right\rangle_{\mathrm{A}}, \left|\mathrm{L}\right\rangle_{\mathrm{A}}\}$, she prepares $\sigma_{j,1}^{\mathrm{R}}$ or $\sigma_{j,1}^{\mathrm{L}}$ at random, while if she measures it in the test basis $\{\left|\mathrm{H}\right\rangle_{\mathrm{A}}, \left|\mathrm{V}\right\rangle_{\mathrm{A}}\}$, she prepares $\left|\mathrm{H}\right\rangle_{\mathrm{B}}$ or $\left|\mathrm{V}\right\rangle_{\mathrm{B}}$ at random independently of $j \in \Gamma^{\mathrm{key}}$. As a consequence, for all $j \in \Gamma^{\mathrm{key}}$, the phase-error rate (PHER) of $\sigma_{j,1}^{\mathrm{R}}$ and $\sigma_{j,1}^{\mathrm{L}}$ could be estimated from the bit-error rate (BER) of the pure states $\left|\mathrm{H}\right\rangle_{\mathrm{B}}$ and $\left|\mathrm{V}\right\rangle_{\mathrm{B}}$ (for a formal definition of the PHER, see Appendix C). Indeed, by postselecting the test regions Ω_j^{H} and Ω_j^{V} of Eq. (5), such perfect states are actually prepared at a certain rate, because the single-photon components of σ_j^{H} and σ_j^{V} verify

$$\begin{aligned} \sigma_{j,1}^{\mathrm{H}} &= \lambda_j^{\mathrm{test}} \left|\mathrm{H}\right\rangle \left\langle \mathrm{H}\right| + (1-\lambda_j^{\mathrm{test}}) \frac{\mathbb{1}}{2}, \\ \sigma_{j,1}^{\mathrm{V}} &= \lambda_j^{\mathrm{test}} \left|\mathrm{V}\right\rangle \left\langle \mathrm{V}\right| + (1-\lambda_j^{\mathrm{test}}) \frac{\mathbb{1}}{2}, \end{aligned} \tag{13}$$

for $\lambda_j^{\mathrm{test}} = \langle e^{-I} I \sin\theta \cos\phi \rangle_{\Omega_j^{\mathrm{H}}} \big/ \langle e^{-I} I \rangle_{\Omega_j^{\mathrm{H}}}$ and all $j \in \Gamma^{\mathrm{test}}$. In other words, the postselection of $\sigma_{j,1}^{\mathrm{H}}$ ($\sigma_{j,1}^{\mathrm{V}}$) determines the preparation of the ideal state $\left|\mathrm{H}\right\rangle$ ($\left|\mathrm{V}\right\rangle$) with probability $\lambda_j^{\mathrm{test}}$ and the fully mixed state with probability $1-\lambda_j^{\mathrm{test}}$.

Exploiting this feature, in Sec. VI we provide a decoy-state method that targets the BER of the ideal components $|\mathrm{H}\rangle_{\mathrm{B}}$ and $|\mathrm{V}\rangle_{\mathrm{B}}$ of $\sigma_{j,1}^{\mathrm{H}}$ and $\sigma_{j,1}^{\mathrm{V}}$ directly, rather than the mixed-state BER contemplated in the asymptotic analyses [35,36].

V. PROTOCOL DESCRIPTION

For ease of understanding, we provide a description of a fully passive decoy-state BB84 protocol before explaining our PE method.

For a previously agreed number of rounds N, the parties do the following.

(1) *State preparation.* Alice operates the passive source and verifies if the delivered state matches any acceptance region. Namely, she reads the outcomes ϕ, θ, and I from her measurement unit to check if $(\phi, \theta, I) \in \Omega_j^{\mathrm{R(L)}}$ for some $j \in \Gamma^{\mathrm{key}}$, or if $(\phi, \theta, I) \in \Omega_j^{\mathrm{H(V)}}$ for some $j \in \Gamma^{\mathrm{test}}$.

(2) *Measurement.* Bob measures the incoming signal in the β basis with probability q_β, $\beta \in \{\mathrm{key}, \mathrm{test}\}$.

After the quantum communication phase, the public discussion and the classical postprocessing run as follows.

(3) *Public discussion.* For each basis β and decoy setting $j \in \Gamma^\beta$, Alice communicates to Bob the set of rounds where σ_j^β was postselected (i.e., where the acceptance region Ω_j^β was recorded). In return, Bob reveals to Alice the subsets of these sets where a basis match occurred and a detection event was recorded, say, $\{\mathcal{X}_j^\beta\}_{j\in\Gamma^\beta}$. The corresponding "numbers of counts" are denoted by $M_j^\beta = |\mathcal{X}_j^\beta|$ and $\mathcal{X}^{\mathrm{key}} = \bigcup_{j\in\Gamma^{\mathrm{key}}} \mathcal{X}_j^{\mathrm{key}}$ $(\mathcal{X}^{\mathrm{test}} = \bigcup_{j\in\Gamma^{\mathrm{test}}} \mathcal{X}_j^{\mathrm{test}})$ identifies the sifted-key data (the test-basis PE data). Lastly, Alice discloses her bit strings for the test sets $\mathcal{X}_j^{\mathrm{test}}$.

(4) *Parameter estimation.* Comparing Alice's test bit strings with his own, Bob computes the corresponding "numbers of error counts," say, $\{m_j^{\mathrm{test}}\}_{j\in\Gamma^{\mathrm{test}}}$. From his available data, Bob estimates a lower bound, $M_{\mathrm{key},1}^{\mathrm{L}}$, on the number of single-photon counts in $\mathcal{X}^{\mathrm{key}}$, $M_{\mathrm{key},1}$ and an upper bound, $e_1^{(\mathrm{ph})\ \mathrm{U}}$, on the single-photon PHER in this set, $e_1^{(\mathrm{ph})}$. Bob uses the above bounds to compute the secret-key length, l, for a prefixed error-correction (EC) leakage, λ_{EC}, and a prefixed error verification (EV) tag size, $\lceil \log(1/\epsilon_{\mathrm{cor}}) \rceil$. If $l = 0$, Bob aborts the protocol.

(5) *Error correction and error verification.* Upon success of the PE step, the parties run the previously agreed EC and EV steps, the latter being based on two-universal hashing [47]. If EV fails, Bob aborts the protocol.

(6) *Privacy amplification.* Upon success of the EV step, the parties apply privacy amplification (PA) based on two-universal hashing [47,48] to their reconciled sifted keys, obtaining final keys of length l.

For a derivation of the secret-key length l, see Appendix C.

On another note, we remark that, for ease of understanding, the above protocol description presumes that Alice postselects the acceptance regions on a round-by-round basis. In a practical implementation though, this postselection would be done after the quantum communication, using the transcript of measurement outcomes recorded by Alice's measurement unit.

To end this section, we include a back-up table (Table I) summarizing the main protocol sets and parameters.

VI. DECOY-STATE METHOD

Here, we generalize the decoy-state method of Ref. [36] to the finite-key regime, incorporating methodology that surpasses a limitation of both [35,36].

We recall that following the adversary model of Sec. II, the state of Eve's register at the end of round $u-1$, R_{u-1}, fully determines Eve's intervention in round u. This said, the notation goes as follows. For $u = 1, 2 \dots N$, $Q_j^{\beta(u)}$ $(E_j^{\beta(u)})$ denotes the probability that a "click" (an "error") is recorded in round u, conditioned on R_{u-1} and on the event that σ_j^β is postselected, and Bob performs a β-basis measurement, $\beta \in \{\mathrm{key}, \mathrm{test}\}$.

TABLE I. The protocol sets and notation.

N	Number of protocol rounds
q_β	Bob's β-basis probability, $\beta \in \{\mathrm{key}, \mathrm{test}\}$
Γ^β	List of β-basis decoy settings
Ω_j^{R}, Ω_j^{L}	Elementary key-basis postselection regions with decoy setting $j \in \Gamma^{\mathrm{key}}$
Ω_j^{key}	$\Omega_j^{\mathrm{R}} \cup \Omega_j^{\mathrm{L}}$
Ω_j^{H}, Ω_j^{V}	Elementary test-basis postselection regions with decoy setting $j \in \Gamma^{\mathrm{test}}$
Ω_j^{test}	$\Omega_j^{\mathrm{H}} \cup \Omega_j^{\mathrm{V}}$
Ω^β	$\bigcup_{j\in\Gamma^\beta} \Omega_j^\beta$
$\mathcal{X}_j^\beta$	Set of rounds where Ω_j^β is postselected, a basis match occurs, and a click is recorded
$\mathcal{X}^\beta$	$\bigcup_{j\in\Gamma^\beta} \mathcal{X}_j^\beta$
M_j^β	$\lvert\mathcal{X}_j^\beta\rvert$
m_j^{test}	Number of error counts in $\mathcal{X}_j^{\mathrm{test}}$
$M_{\mathrm{key},1}^{\mathrm{L}}$	Lower bound on the number $M_{\mathrm{key},1}$ of single-photon counts in $\mathcal{X}^{\mathrm{key}}$
$e_1^{(\mathrm{ph})\ \mathrm{U}}$	Upper bound on the rate $e_1^{(\mathrm{ph})}$ of single-photon phase errors in $\mathcal{X}^{\mathrm{key}}$
l	Secret-key length
λ_{EC}	Error-correction leakage

That is to say, $Q_j^{\beta(u)} = p^{(u)}\big(\text{click}|R_{u-1},\sigma_j^{\beta},\beta\big)$ and $E_j^{\beta(u)} = p^{(u)}\big(\text{error}|R_{u-1},\sigma_j^{\beta},\beta\big)$. Similarly, $y_{j,n}^{\beta(u)}$ and $e_{j,n}^{\beta(u)}$ denote the corresponding n-photon yield and n-photon error probability, $y_{j,n}^{\beta(u)} = p^{(u)}\big(\text{click}|R_{u-1},\sigma_{j,n}^{\beta},\beta\big)$ and $e_{j,n}^{\beta(u)} = p^{(u)}\big(\text{error}|R_{u-1},\sigma_{j,n}^{\beta},\beta\big)$. Note that "error" refers here to the joint event where a click is recorded and it triggers a bit error.

A. Decoy constraints

From the photon-number decomposition of σ_j^{β}, it follows that $Q_j^{\beta(u)} = \sum_{n=0}^{\infty} p_{n|j}^{\beta} y_{j,n}^{\beta(u)}$ and $E_j^{\beta(u)} = \sum_{n=0}^{\infty} p_{n|j}^{\beta}$ $e_{j,n}^{\beta(u)}$ for all $u = 1,2\ldots N$, $j \in \Gamma^{\beta}$ and $\beta \in \{\text{key},\text{test}\}$. If we now define the averaged quantities $Q_j^{\beta} = \sum_u Q_j^{\beta(u)}/N$, $E_j^{\beta} = \sum_u E_j^{\beta(u)}/N$, $y_{j,n}^{\beta} = \sum_u y_{j,n}^{\beta(u)}/N$ and $e_{j,n}^{\beta} = \sum_u$ $e_{j,n}^{\beta(u)}/N$, and truncate the index n to a threshold photon number n_{cut}, we derive the sets of constraints

$$\begin{aligned} Q_j^{\beta} &\geq \sum_{n=0}^{n_{\text{cut}}} p_{n|j}^{\beta} y_{j,n}^{\beta}, \\ Q_j^{\beta} &\leq \sum_{n=0}^{n_{\text{cut}}} p_{n|j}^{\beta} y_{j,n}^{\beta} + 1 - \sum_{n=0}^{n_{\text{cut}}} p_{n|j}^{\beta}, \end{aligned} \tag{14}$$

and

$$\begin{aligned} E_j^{\beta} &\geq \sum_{n=0}^{n_{\text{cut}}} p_{n|j}^{\beta} e_{j,n}^{\beta}, \\ E_j^{\beta} &\leq \sum_{n=0}^{n_{\text{cut}}} p_{n|j}^{\beta} e_{j,n}^{\beta} + 1 - \sum_{n=0}^{n_{\text{cut}}} p_{n|j}^{\beta}, \end{aligned} \tag{15}$$

to be addressed numerically later on.

B. Trace-distance constraints

Next, we reproduce the TD constraints provided in Ref. [36], to be combined with the above decoy constraints. For each basis β and photon number n, these extra constraints restrict the differences $|y_{j,n}^{\beta} - y_{k,n}^{\beta}|$ and $|e_{j,n}^{\beta} - e_{k,n}^{\beta}|$ for every pair of distinct settings (j,k).

1. Yields

Regarding the yields, Bob's possible measurement outcomes are "click" and "no click," such that his measurement can be described by a positive-operator-valued measure (POVM) with elements $\{\hat{M}_{\text{B}}^{\text{click}}, \hat{M}_{\text{B}}^{\text{no click}}\}$, where $\hat{M}_{\text{B}}^{\text{no click}} = \mathbb{1}_{\text{B}} - \hat{M}_{\text{B}}^{\text{click}}$ (note that this POVM is basis independent due to the basis-independent detection-efficiency assumption). Therefore, from the adversary model described in Sec. II, we have that

$$y_{j,n}^{\beta(u)} = \text{Tr}\left[\hat{D}_{\text{BE}}^{\text{click}(u)}\, \sigma_{j,n}^{\beta} \otimes \xi_{\text{E}}^{(u)}\right], \tag{16}$$

for $\hat{D}_{\text{BE}}^{\text{click}(u)} = \hat{U}_{\text{BE}}^{(u)\dagger} \hat{M}_{\text{B}}^{\text{click}} \hat{U}_{\text{BE}}^{(u)}$, where $\xi_{\text{E}}^{(u)}$ and $\hat{U}_{\text{BE}}^{(u)}$, respectively, denote the state of Eve's quantum probe and Eve's unitary operation in round u.

Now, by virtue of the TD argument presented in Appendix A, it follows that

$$|y_{j,n}^{\beta(u)} - y_{k,n}^{\beta(u)}| \leq D\left(\sigma_{j,n}^{\beta}, \sigma_{k,n}^{\beta}\right), \tag{17}$$

for all possible inputs β, j, k, n and u, where $D(\rho,\tau) = \frac{1}{2}\text{Tr}[\sqrt{(\rho-\tau)^2}]$ denotes the TD between ρ and τ. In particular, we remark that $\sigma_{j,1}^{\text{key}} = \mathbb{1}/2$ ($\sigma_{j,0}^{\text{key}} = |\text{vac}\rangle\langle\text{vac}|$) for all $j \in \Gamma^{\text{key}}$ and $\sigma_{j,1}^{\text{test}} = \mathbb{1}/2$ ($\sigma_{j,0}^{\text{test}} = |\text{vac}\rangle\langle\text{vac}|$) for all $j \in \Gamma^{\text{test}}$ [see Eqs. (9) and (13)]. As a consequence, the single-photon yield and the vacuum yield are independent of both the intensity setting and the basis.

2. Test-basis error probabilities

In order to describe the test-basis error probabilities, finer-grained measurement operators are required, in a one-to-one correspondence with Bob's possible outcomes: "H," "V," and "no click". As usual, double clicks are randomly assigned to either "H" or "V" and this assignment is straightforwardly incorporated in the POVM. In short, error-wise, Bob's measurement is described by a POVM with elements $\{\hat{M}_{\text{B}}^{\text{H}}, \hat{M}_{\text{B}}^{\text{V}}, \hat{M}_{\text{B}}^{\text{noclick}}\}$, where $\hat{M}_{\text{B}}^{\text{H}} + \hat{M}_{\text{B}}^{\text{V}} = \hat{M}_{\text{B}}^{\text{click}}$. Moreover, since $\sigma_{j,n}^{\text{test}} = \big(\sigma_{j,n}^{\text{H}} + \sigma_{j,n}^{\text{V}}\big)/2$ it follows that

$$\begin{aligned} e_{j,n}^{\text{test}(u)} &= \frac{1}{2}\Big[p^{(u)}\left(\text{V}|R_{u-1},\sigma_{j,n}^{\text{H}},\text{test}\right) \\ &\quad + p^{(u)}\left(\text{H}|R_{u-1},\sigma_{j,n}^{\text{V}},\text{test}\right)\Big] \\ &= \frac{1}{2}\Big\{\text{Tr}\left[\hat{D}_{\text{BE}}^{\text{V}(u)}\, \sigma_{j,n}^{\text{H}} \otimes \xi_{\text{E}}^{(u)}\right] \\ &\quad + \text{Tr}\left[\hat{D}_{\text{BE}}^{\text{H}(u)}\, \sigma_{j,n}^{\text{V}} \otimes \xi_{\text{E}}^{(u)}\right]\Big\}, \end{aligned} \tag{18}$$

for $\hat{D}^{y(u)} = \hat{U}_{\text{BE}}^{(u)\dagger} \hat{M}_{\text{B}}^{y} \hat{U}_{\text{BE}}^{(u)}$ with $y \in \{\text{H},\text{V}\}$. Next, by combining the TD argument with the triangle inequality, one can readily show that

$$\left|e_{j,n}^{\text{test}(u)} - e_{k,n}^{\text{test}(u)}\right| \leq \frac{1}{2}\left[D\left(\sigma_{j,n}^{\text{H}}, \sigma_{k,n}^{\text{H}}\right) + D\left(\sigma_{j,n}^{\text{V}}, \sigma_{k,n}^{\text{V}}\right)\right]. \tag{19}$$

Moreover, because of the azimuthal symmetry of the output state of the source, $D\big(\sigma_{j,n}^{\text{H}}, \sigma_{k,n}^{\text{H}}\big) = D\big(\sigma_{j,n}^{\text{V}}, \sigma_{k,n}^{\text{V}}\big)$ and thus

$$\left| e^{\text{test}(u)}_{j,n} - e^{\text{test}(u)}_{k,n} \right| \leq D\left(\sigma^{\mathrm{H}}_{j,n}, \sigma^{\mathrm{H}}_{k,n}\right). \tag{20}$$

In particular, $e^{\text{test}(u)}_{j,0} = e^{\text{test}(u)}_{k,0}$ for all j and k but $e^{\text{test}(u)}_{j,1} \neq e^{\text{test}(u)}_{k,1}$ because $\sigma^{\mathrm{H}}_{j,1} \neq \sigma^{\mathrm{H}}_{k,1}$ if $j \neq k$.

Since the TD bounds in Eqs. (17) and (20) are round independent, the exact same bounds hold after averaging over all protocol rounds (this is an immediate consequence of the triangle inequality too). That is to say, $|y^{\beta}_{j,n} - y^{\beta}_{k,n}| \leq D(\sigma^{\beta}_{j,n}, \sigma^{\beta}_{k,n})$ for $\beta \in \{\text{key}, \text{test}\}$, and $|e^{\text{test}}_{j,n} - e^{\text{test}}_{k,n}| \leq D(\sigma^{\mathrm{H}}_{j,n}, \sigma^{\mathrm{H}}_{k,n})$ for all possible j, k and n. In order to explicitly calculate these TD values, we use the matrix representation described in Appendix B.

C. Noise-suppressing constraints

As shown in Sec. IV, the BER of the ideal states $|\mathrm{H}\rangle$ and $|\mathrm{V}\rangle$ is the relevant quantity to estimate the PHER of the key-generating states $\sigma^{\mathrm{R}}_{j,1}$ and $\sigma^{\mathrm{L}}_{j,1}$ and one can target this quantity directly in the LP by harnessing Eq. (13). This is what we do next.

By plugging Eq. (13) into Eq. (18) and using (i) $\hat{D}^{\mathrm{H}(u)}_{\mathrm{BE}} + \hat{D}^{\mathrm{V}(u)}_{\mathrm{BE}} = \hat{D}^{\text{click}(u)}_{\mathrm{BE}}$ and (ii) $\mathbb{1}/2 = \sigma^{\text{test}}_{j,1}$, one obtains

$$\begin{aligned} e^{\text{test}(u)}_{j,1} &= \lambda^{\text{test}}_j \frac{\mathrm{Tr}\left[\hat{D}^{\mathrm{V}(u)}_{\mathrm{BE}} \left|\mathrm{H}\right\rangle \left\langle\mathrm{H}\right| \otimes \xi^{(u)}_{\mathrm{E}}\right] + \mathrm{Tr}\left[\hat{D}^{\mathrm{H}(u)}_{\mathrm{BE}} \left|\mathrm{V}\right\rangle \left\langle\mathrm{V}\right| \otimes \xi^{(u)}_{\mathrm{E}}\right]}{2} \\ &\quad + (1-\lambda^{\text{test}}_j)\frac{\mathrm{Tr}\left[\hat{D}^{\mathrm{V}(u)}_{\mathrm{BE}} \frac{\mathbb{1}}{2} \otimes \xi^{(u)}_{\mathrm{E}}\right] + \mathrm{Tr}\left[\hat{D}^{\mathrm{H}(u)}_{\mathrm{BE}} \frac{\mathbb{1}}{2} \otimes \xi^{(u)}_{\mathrm{E}}\right]}{2} \\ &= \lambda^{\text{test}}_j \frac{p^{(u)}\left(\mathrm{V}|R_{u-1}, \left|\mathrm{H}\right\rangle\left\langle\mathrm{H}\right|, \text{test}\right) + p^{(u)}\left(\mathrm{H}|R_{u-1}, \left|\mathrm{V}\right\rangle\left\langle\mathrm{V}\right|, \text{test}\right)}{2} + (1-\lambda^{\text{test}}_j)\frac{p^{(u)}\left(\text{click}|R_{u-1}, \sigma^{\text{test}}_{j,1}, \text{test}\right)}{2}. \end{aligned} \tag{21}$$

By definition, the first term is the contribution of the ideal states $|\mathrm{H}\rangle$ and $|\mathrm{V}\rangle$ to the conditional bit-error probability in round u, say, $e^{\text{ideal}(u)}_{1}$, and the second term is the white-noise contribution from the fully mixed state. Noting that $p^{(u)}\left(\text{click}|R_{u-1}, \sigma^{\text{test}}_{j,1}, \text{test}\right) = y^{\text{test}(u)}_{j,1}$, Eq. (21) reads $e^{\text{test}(u)}_{j,1} = \lambda^{\text{test}}_j e^{\text{ideal}(u)}_{1} + (1-\lambda^{\text{test}}_j) y^{\text{test}(u)}_{j,1}/2$, which leads to

$$e^{\text{test}}_{j,1} = \lambda^{\text{test}}_j e^{\text{ideal}}_{1} + (1-\lambda^{\text{test}}_j)\frac{y^{\text{test}}_{j,1}}{2} \tag{22}$$

for the averaged quantities $e^{\text{test}}_{j,1} = \sum_u e^{\text{test}(u)}_{j,1}/N$, $e^{\text{ideal}}_{1} = \sum_u e^{\text{ideal}(u)}_{1}/N$ and $y^{\text{test}}_{j,1} = \sum_u y^{\text{test}(u)}_{j,1}/N$. We remark that the white-noise component $y^{\text{test}}_{j,1}/2$ is setting independent (just like the ideal component e^{ideal}_{1}) due to the setting independence of $y^{\text{test}}_{j,1}$.

D. Linear programs

Here, we select an arbitrary reference setting $\alpha \in \Gamma^{\text{key}}$, such that $y^{\text{key}}_{\alpha,1}$ becomes the target of the yield-related linear program (LP). Of course, by virtue of the setting independence and the basis independence of the single-photon yield, one could select a different setting from Γ^{key} or even from Γ^{test} for this purpose.

Combining the three types of constraints we have presented, one reaches final LPs for the estimation of the single-photon parameters $y^{\text{key}}_{\alpha,1}$ and e^{ideal}_{1} given $\{Q^{\text{key}}_j\}_{j\in\Gamma^{\text{key}}}$ and $\{E^{\text{test}}_j\}_{j\in\Gamma^{\text{test}}}$. Note, however, that the latter cannot be determined with certainty in the protocol but only estimated from the observed numbers of key-basis measure counts, $\{M^{\text{key}}_j\}_{j\in\Gamma^{\text{key}}}$, and test-basis error counts, $\{m^{\text{test}}_j\}_{j\in\Gamma^{\text{test}}}$, using concentration inequalities for sums of dependent random variables (RVs). In particular, we use Kato's inequality [44] for this purpose, which allows one to establish that

$$\begin{aligned} N q_{\text{key}} \left\langle 1\right\rangle_{\Omega^{\text{key}}_j} Q^{\text{key}}_j &\overset{2\epsilon}{\in} \left(K^{\mathrm{L}}_{N,\epsilon}(M^{\text{key}}_j), K^{\mathrm{U}}_{N,\epsilon}(M^{\text{key}}_j)\right), \\ N q_{\text{test}} \left\langle 1\right\rangle_{\Omega^{\text{test}}_j} E^{\text{test}}_j &\overset{2\epsilon}{\in} \left(K^{\mathrm{L}}_{N,\epsilon}(m^{\text{test}}_j), K^{\mathrm{U}}_{N,\epsilon}(m^{\text{test}}_j)\right), \end{aligned} \tag{23}$$

for known functions $K^{\mathrm{L}}_{N,\epsilon}(x)$ and $K^{\mathrm{U}}_{N,\epsilon}(x)$ given in Appendix D, where the superscripts 2ϵ over the "$\in$" symbols indicate that the corresponding intervals hold except with probability 2ϵ at most [49]. To be precise, in both intervals of Eq. (23), each one-sided bound holds except with probability ϵ at most, which translates into an overall error probability of 2ϵ by virtue of the union bound [50]. As an example, for the explicit derivation of one of the bounds in Eq. (23), see Appendix E.

In conclusion, we can take $\{Q_j^{\rm key}\}_{j\in\Gamma^{\rm key}}$ and $\{E_j^{\rm test}\}_{j\in\Gamma^{\rm test}}$ to be additional variables of the LPs, as long as we further incorporate the constraints set by Eq. (23) [51]. Putting all this together, if one denotes $|\Gamma^{\rm key}| = d_{\rm key}$ and $|\Gamma^{\rm test}| = d_{\rm test}$, it follows that

$$y_{\alpha,1}^{\rm key} \overset{2\epsilon d_{\rm key}}{>} y_1^{\rm L} \text{ and } e_1^{\rm ideal} \overset{2\epsilon(d_{\rm key}+d_{\rm test})}{<} e_1^{\rm idealU} \tag{24}$$

(the superscripts upper bounding the error probabilities again), where $y_1^{\rm L}$ is the solution to

$$\begin{aligned}
&\min \quad y_{\alpha,1}^{\rm key} \quad \text{such that}\\
&\sum_{n=0}^{n_{\rm cut}} p_{n|j}^{\rm key} y_{j,n}^{\rm key} \leq Q_j^{\rm key},\ j \in \Gamma^{\rm key},\\
&Q_j^{\rm key} \leq \sum_{n=0}^{n_{\rm cut}} p_{n|j}^{\rm key} y_{j,n}^{\rm key} + 1 - \sum_{n=0}^{n_{\rm cut}} p_{n|j}^{\rm key},\ j \in \Gamma^{\rm key},\\
&\left|y_{j,n}^{\rm key} - y_{k,n}^{\rm key}\right| \leq D\big(\sigma_{j,n}^{\rm key}, \sigma_{k,n}^{\rm key}\big),\ j,k \in \Gamma^{\rm key},\ n = 2\ldots n_{\rm cut},\\
&y_{j,n}^{\rm key} = y_{k,n}^{\rm key},\ j,k \in \Gamma^{\rm key},\ n = 0,1,\\
&0 \leq y_{j,n}^{\rm key} \leq 1,\ j \in \Gamma^{\rm key},\ n = 0\ldots n_{\rm cut},\\
&\frac{K_{N,\epsilon}^{\rm L}(M_j^{\rm key})}{N q_{\rm key} \langle 1\rangle_{\Omega_j^{\rm key}}} \leq Q_j^{\rm key} \leq \frac{K_{N,\epsilon}^{\rm U}(M_j^{\rm key})}{N q_{\rm key} \langle 1\rangle_{\Omega_j^{\rm key}}},\ j \in \Gamma^{\rm key},
\end{aligned} \tag{25}$$

and $e_1^{\rm idealU}$ is the solution to

$$\begin{aligned}
&\max \quad e_1^{\rm ideal} \quad \text{such that}\\
&\sum_{n=0}^{n_{\rm cut}} p_{n|j}^{\rm test} e_{j,n}^{\rm test} \leq E_j^{\rm test},\ j \in \Gamma^{\rm test},\\
&E_j^{\rm test} \leq \sum_{n=0}^{n_{\rm cut}} p_{n|j}^{\rm test} e_{j,n}^{\rm test} + 1 - \sum_{n=0}^{n_{\rm cut}} p_{n|j}^{\rm test},\ j \in \Gamma^{\rm test},\\
&\left|e_{j,n}^{\rm test} - e_{k,n}^{\rm test}\right| \leq D\big(\sigma_{j,n}^{\rm H}, \sigma_{k,n}^{\rm H}\big),\ j,k \in \Gamma^{\rm test},\ n = 1\ldots n_{\rm cut},\\
&e_{j,0}^{\rm test} = e_{k,0}^{\rm test},\ j,k \in \Gamma^{\rm test},\\
&\lambda_j^{\rm test} e_1^{\rm ideal} \leq e_{j,1}^{\rm test} - (1-\lambda_j^{\rm test})\frac{y_1^{\rm L}}{2},\ j \in \Gamma^{\rm test},\\
&0 \leq e_1^{\rm ideal} \leq 1,\ 0 \leq e_{j,n}^{\rm test} \leq 1,\ j \in \Gamma^{\rm test},\ n = 0\ldots n_{\rm cut},\\
&\frac{K_{N,\epsilon}^{\rm L}(m_j^{\rm test})}{N q_{\rm test} \langle 1\rangle_{\Omega_j^{\rm test}}} \leq E_j^{\rm test} \leq \frac{K_{N,\epsilon}^{\rm U}(m_j^{\rm test})}{N q_{\rm test} \langle 1\rangle_{\Omega_j^{\rm test}}},\ j \in \Gamma^{\rm test}.
\end{aligned} \tag{26}$$

Note that the error probability of the first LP is bounded by $2\epsilon d_{\rm key}$ because it relies on $2\epsilon d_{\rm key}$ usages of Kato's inequality for the measure counts $\{M_j^{\rm key}\}_{j\in\Gamma^{\rm key}}$, each of them having a fixed error probability ϵ. On the contrary, the second LP has an error probability of $2\epsilon(d_{\rm key}+d_{\rm test})$ because, besides relying on $2\epsilon d_{\rm test}$ usages of Kato's inequality for the error counts $\{m_j^{\rm test}\}_{j\in\Gamma^{\rm test}}$, it further uses the fact that, for all $j \in \Gamma^{\rm test}$, $y_{j,1}^{\rm test} = y_{\alpha,1}^{\rm key} \overset{2\epsilon d_{\rm key}}{>} y_1^{\rm L}$.

Alternatively, running the first LP under a maximization condition instead provides an upper bound $y_1^{\rm U}$ on $y_{\alpha,1}^{\rm key}$, such that $y_{\alpha,1}^{\rm key} \overset{2\epsilon d_{\rm key}}{<} y_1^{\rm U}$.

VII. SECRET-KEY PARAMETERS

In order to evaluate the secret-key-length formula, given by Eq. (C2), one must estimate the secret-key parameters $M_{\rm key,1}$ and $e_1^{\rm (ph)}$. This is what we do next, using the decoy-state bounds $y_1^{\rm L}$, $y_1^{\rm U}$ and $e_1^{\rm idealU}$.

For simplicity, a common error probability ϵ will be assumed for every usage of a concentration inequality in what follows, matching the error probability presumed for the Kato bounds in the previous section.

A. Bounds on the single-photon measure counts

Let us introduce the notation $\Omega^\beta = \bigcup_{j\in\Gamma^\beta}\Omega_j^\beta$ for $\beta \in \{\text{key}, \text{test}\}$. From the reverse Kato bounds of Appendix D and an argument formally identical to that of Appendix E (but applied to a different sequence of Bernoulli RVs), one can show that

$$\begin{aligned}
M_{\rm key,1} \overset{2\epsilon}{\in} \Big(&\bar{K}_{N,\epsilon}^{\rm L}\Big(N q_{\rm key} \langle e^{-I} I\rangle_{\Omega^{\rm key}} y_{\alpha,1}^{\rm key}\Big),\\
&\bar{K}_{N,\epsilon}^{\rm U}\Big(N q_{\rm key} \langle e^{-I} I\rangle_{\Omega^{\rm key}} y_{\alpha,1}^{\rm key}\Big)\Big),
\end{aligned} \tag{27}$$

for known functions $\bar{K}_{N,\epsilon}^{\rm L}(x)$ and $\bar{K}_{N,\epsilon}^{\rm U}(x)$ given in Appendix D. As in Eq. (23), each bound in the interval above holds except with probability ϵ at most. Also, we remark that Eq. (27) explicitly uses the fact that $y_{j,1}^{\rm key} = y_{\alpha,1}^{\rm key}$ for all $j \in \Gamma^{\rm key}$. Now, using $y_{\alpha,1}^{\rm key} \overset{2\epsilon d_{\rm key}}{>} y_1^{\rm L}$ and $y_{\alpha,1}^{\rm key} \overset{2\epsilon d_{\rm key}}{<} y_1^{\rm U}$ in Eq. (27), it follows that

$$\begin{aligned}
M_{\rm key,1} &\overset{\epsilon(2d_{\rm key}+1)}{>} \bar{K}_{N,\epsilon}^{\rm L}\Big(N q_{\rm key} \langle e^{-I} I\rangle_{\Omega^{\rm key}} y_1^{\rm L}\Big) =: M_{\rm key,1}^{\rm L},\\
M_{\rm key,1} &\overset{\epsilon(2d_{\rm key}+1)}{<} \bar{K}_{N,\epsilon}^{\rm U}\Big(N q_{\rm key} \langle e^{-I} I\rangle_{\Omega^{\rm key}} y_1^{\rm U}\Big) =: M_{\rm key,1}^{\rm U}.
\end{aligned} \tag{28}$$

In a similar fashion, one can derive a lower bound on the number of measure counts in $\mathcal{X}^{\rm test}$ triggered by the perfectly prepared test states $|{\rm H}\rangle$ and $|{\rm V}\rangle$, say, $M_{\rm test,1}^{\rm ideal}$. This is so because $(|{\rm H}\rangle\langle{\rm H}| + |{\rm V}\rangle\langle{\rm V}|)/2 = \sigma_{\alpha,1}^{\rm key} = \mathbb{1}/2$ and hence $y_1^{\rm L}$ provides a lower bound on the corresponding average yield too ($y_1^{\rm L}$ lower bounds the round-averaged yield of any convex combination of single-photon states that adds up to $\mathbb{1}/2$). In particular, we have

$$M^{\text{ideal}}_{\text{test},1} \overset{\epsilon(2d_{\text{key}}+1)}{>} \bar{K}^{\text{L}}_{N,\epsilon}\left(Nq_{\text{test}}\left\langle e^{-I}I\right\rangle_{\Omega^{\text{test}}}\lambda^{\text{test}}y_1^{\text{L}}\right) =: M^{\text{ideal L}}_{\text{test},1}, \tag{29}$$

where we have introduced $\lambda^{\text{test}} = \langle e^{-I}I\sin\theta\cos\phi\rangle_{\Omega^{\text{H}}} / \langle e^{-I}I\rangle_{\Omega^{\text{H}}}$ for $\Omega^{\text{H}} = \bigcup_{j\in\Gamma^{\text{test}}}\Omega_j^{\text{H}}$.

B. Upper bound on the phase-error rate

Once again, from a reverse Kato bound of Appendix D and an argument formally identical to that of Appendix E, one can establish that the number $m^{\text{ideal}}_{\text{test},1}$ of single-photon error counts in $\mathcal{X}^{\text{test}}$ triggered by perfectly prepared states satisfies

$$m^{\text{ideal}}_{\text{test},1} \overset{\epsilon[2(d_{\text{key}}+d_{\text{test}})+1]}{<} \bar{K}^{\text{U}}_{N,\epsilon}\left(Nq_{\text{test}}\left\langle e^{-I}I\right\rangle_{\Omega^{\text{test}}}\lambda^{\text{test}}e_1^{\text{idealU}}\right) =: m^{\text{ideal U}}_{\text{test},1}, \tag{30}$$

where the error term $\epsilon[2(d_{\text{key}}+d_{\text{test}})+1]$ arises from the usual composition of errors.

Let us now derive an upper bound on the single-photon PHER $e_1^{(\text{ph})} = m^{(\text{ph})}_{\text{key},1}/M_{\text{key},1}$, where $m^{(\text{ph})}_{\text{key},1}$ is the RV describing the number of single-photon phase errors in $\mathcal{X}^{\text{key}}$. As found in Sec. IV, these errors would arise from uniformly preparing $|\text{H}\rangle$ and $|\text{V}\rangle$ and measuring them in the test basis, which means that the ratio $m^{\text{ideal}}_{\text{test},1}/M^{\text{ideal}}_{\text{test},1}$ is an unbiased estimator of $e_1^{(\text{ph})}$ by virtue of the standard random sampling argument invoked in the ideal BB84 protocol. To be precise, it follows from Serfling's inequality [52] that

$$m^{(\text{ph})}_{\text{key},1} \overset{\epsilon}{<} m^{\text{ideal}}_{\text{test},1}\frac{M_{\text{key},1}}{M^{\text{ideal}}_{\text{test},1}} + \Upsilon\left(M_{\text{key},1}, M^{\text{ideal}}_{\text{test},1}, \epsilon\right), \tag{31}$$

for $\Upsilon(x,y,z) = \sqrt{(x+y)x(y+1)\ln\left(z^{-1}\right)/2y^2}$. Now, making monotonicity considerations separately for each term in the right-hand side of Eq. (31), it follows that

$$m^{(\text{ph})}_{\text{key},1} \overset{\epsilon[2(d_{\text{key}}+d_{\text{test}})+4]}{<}, \quad m^{\text{idealU}}_{\text{test},1}\frac{M^{\text{U}}_{\text{key},1}}{M^{\text{ideal L}}_{\text{test},1}} + \Upsilon\left(M^{\text{U}}_{\text{key},1}, M^{\text{ideal L}}_{\text{test},1}, \epsilon\right) =: m^{(\text{ph})U}_{\text{key},1}, \tag{32}$$

where the usual composition of errors is applied as well. Consequently, the desired bound on the PHER is

$$e_1^{(\text{ph})} \overset{\epsilon[2(d_{\text{key}}+d_{\text{test}})+5]}{<} \frac{m^{(\text{ph})U}_{\text{key},1}}{M^{\text{L}}_{\text{key},1}} =: e_1^{(\text{ph})\text{ U}}, \tag{33}$$

$M^{\text{L}}_{\text{key},1}$ being given in Eq. (28). To sum up, the error bound in Eq. (33), which matches the overall PE error, $\epsilon_{\text{PE}} = \epsilon[2(d_{\text{key}}+d_{\text{test}})+5]$, includes $2(d_{\text{key}}+d_{\text{test}})$ direct Kato bounds for the gains $\{Q_j^{\text{key}}\}_{j\in\Gamma^{\text{key}}}$ and the error gains $\{E_j^{\text{test}}\}_{j\in\Gamma^{\text{test}}}$, four reverse Kato bounds for $M^{\text{L}}_{\text{key},1}$, $M^{\text{U}}_{\text{key},1}$, $M^{\text{ideal L}}_{\text{test},1}$, and $m^{\text{ideal U}}_{\text{test},1}$, and one Serfling bound for $e_1^{(\text{ph})\text{U}}$.

VIII. PERFORMANCE

In this section, we illustrate the rate-distance performance of the proposed passive protocol. The secret-key rate is defined as $K = \max\{l, 0\}/N$, where we recall that the key length l is calculated according to Eq. (C2).

In the absence of experimental data, we consider a standard channel and detector model given in Appendix F, specified by the overall detection efficiency of the system, η, and the dark count probability of Bob's detectors, p_{d}. The η parameter factors as $\eta = \eta_{\text{Bob}}\eta_{\text{ch}}$, where η_{Bob} denotes the detection efficiency of Bob's detectors and η_{ch} stands for the channel transmittance, modeled as $\eta_{\text{ch}} = 10^{-\alpha_{\text{att}}L/10}$ in terms of the attenuation coefficient of the channel, α_{att}, and the transmission length, L. For comparison purposes, we use the same values as in Ref. [36]: $\eta_{\text{det}} = 65\%$, $\alpha = 0.2$ dB/km, and $p_{\text{d}} = 10^{-6}$.

The threshold photon number of the LPs is set to $n_{\text{cut}} = 4$, resulting in a negligible loss in performance according to our simulations. For illustration purposes, the numbers of decoy settings are set to $d_{\text{key}} = d_{\text{test}} = 4$, in such a way that we can denote $\Gamma^{\text{key}} = \{\alpha, \beta, \gamma, \delta\}$ and $\Gamma^{\text{test}} = \{\alpha', \beta', \gamma', \delta'\}$. We observe that using four settings instead of three provides a better robustness to loss and we remark that, contrary to what happens with an active setup, increasing the number of decoys does not require to modify the hardware in the passive scenario. To be precise, for the key basis, we select consecutive intervals of the form $I_\delta/4\nu t = [0, w)$, $I_\gamma/4\nu t = [w, 2w)$, $I_\beta/4\nu t = [2w, 3w)$ and $I_\alpha/4\nu t = [3w, 1)$, w denoting a fixed width parameter. For the test basis, we use overlapping intervals instead, i.e., $I_{\delta'}/4\nu t = [0, w)$, $I_{\gamma'}/4\nu t = [0, 2w)$, $I_{\beta'}/4\nu t = [0, 3w)$ and $I_{\alpha'}/4\nu t = [0, 1)$, maintaining the width parameter w for simplicity. Evidence based on multiple numerical trials indicates that the use of overlapping intervals in the test basis seems beneficial but apparently it is not so for the key basis. On top of this, we perform a mild *brute force* optimization in the width parameter, w, the test-basis measurement probability, q_{test}, the output intensity value νt, and the angular widths of the postselection regions, $\Delta\theta'$, $\Delta\theta$, and $\Delta\phi$. In this regard, we recall that a minor advantage may be achieved by using different—or even unconstrained—decoy widths in each basis or further increasing the number of decoys. Notwithstanding, a preliminary analysis seems to indicate that there is not much room for improvement in this respect.

As for the finite-key parameters (introduced in Appendix C), we set the fixed error tolerance of the PE bounds to $\epsilon = 10^{-20}$ and take $\epsilon_{\rm PA} = \delta = \epsilon$, leading to an overall PE error of $\epsilon_{\rm PE} = 21\epsilon$ and a secrecy parameter of $\epsilon_{\rm sec} = \sqrt{\epsilon_{\rm PE}} + \epsilon_{\rm PA} + \delta \approx 4.58 \times 10^{-10}$. The correctness error probability is set to $\epsilon_{\rm cor} = \epsilon = 10^{-20}$ as well. Lastly, all the necessary guesses for Kato's inequality are selected under the assumption of a perfect characterization of the experimental setup. Note, however, that this assumption can be easily removed in practice with a minuscule penalty on the key rate, by carefully modeling the channel or by using the outcomes of previous experiments.

Finally, in order to account for the EC leakage (which would be quantified precisely in a real experiment), we use a standard model described in Appendix F. The model relies on an EC efficiency parameter, $f_{\rm EC}$, which we set to a typical value of $f_{\rm EC} = 1.16$ in the simulations.

The rate-distance plots are shown in Fig. 3, contemplating different numbers of transmission rounds, $N = 10^s$ with $s \in \{9, 10, 11, 12\}$ (dashed light-blue lines) and the asymptotic limit $N \to \infty$ (solid dark-blue line) as well. Since $N \to \infty$ favors arbitrarily small test-basis regions with the considered protocol, in that case we conservatively assume finite minimum sizes $\Delta\theta = \Delta\phi = 0.1$ and $w = 5 \times 10^{-3}$ and optimize the key-basis regions via vt and $\Delta\theta'$ (also, the consideration of overlapping intervals becomes essentially irrelevant in this regime). By doing this, we observe that the asymptotic key rate K_∞ is fairly close to the perfect PE limit (dashed-dotted pink line), in which the estimates of the LPs are replaced by the actual values yielded by the channel model and the key-basis regions are optimized as well. Importantly, the closeness to the perfect PE limit is not a consequence of the noise-suppressing constraints, which only have an (indeed modest) impact in the finite-size secret-key rates—e.g., about a 4% increase for $N = 10^{12}$ and a 16% for $N = 10^9$ in our simulations. Intuitively speaking, the bound on the PHER estimated without any noise suppression at all is already “low enough,” in the sense that further decreasing it (even by orders of magnitude) does not have a great impact on the secret-key rate. Because of this, it is the size of the key regions—which govern the sifting and the BER of the protocol—that essentially determines the secret-key rate.

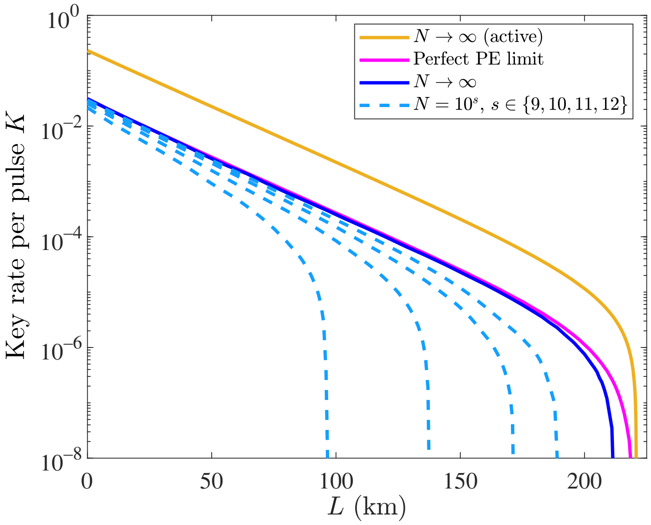

FIG. 3. Rate-distance performance of the fully passive decoy-state BB84 protocol. The finite-key settings, the experimental parameters, and the optimization method are described in the text. Dashed light-blue lines, finite-key regime (N = number of transmission rounds); solid dark-blue line, asymptotic regime; solid pink line, perfect PE limit; solid yellow line, asymptotic performance of an active protocol with three common intensity settings per basis.

For the sake of comparison, we have also plotted K_∞ for a standard active decoy-state BB84 protocol with three common intensity settings per basis (solid yellow line), assuming the same channel model and experimental inputs. The key rate is optimized in the signal and decoy intensities, while the vacuum intensity is set to 10^{-3} for illustration purposes. The figure shows that with the considered protocol design and PE method, the key rate of the active approach only exceeds that of the passive approach by less than one order of magnitude. This feature is further illustrated in Tables II and III, where we compare the finite-key performance of the two approaches for different numbers of signals and transmission distances. For this purpose, in the active protocol we also set $\epsilon_{\rm PA} = \delta = \epsilon_{\rm cor} = \epsilon$ for a fixed error tolerance ϵ of the PE bounds. Nonetheless, since the overall security parameter $\epsilon_{\rm sec}$ +

TABLE II. The active approach for the decoy-state BB84 protocol, as part of a finite-key comparison with the passive approach, shown in Table III.

	N				
L (km)	10^9	10^{10}	10^{11}	10^{12}	∞
0	1.5×10^{-1}	1.8×10^{-1}	2.0×10^{-1}	2.1×10^{-1}	2.3×10^{-1}
40	1.8×10^{-2}	2.4×10^{-2}	2.8×10^{-2}	3.1×10^{-2}	3.6×10^{-2}
80	1.9×10^{-3}	3.0×10^{-3}	3.9×10^{-3}	4.4×10^{-3}	5.8×10^{-3}
120	1.4×10^{-4}	3.2×10^{-4}	4.8×10^{-4}	6.1×10^{-4}	8.8×10^{-4}
160	0	1.7×10^{-5}	4.2×10^{-5}	6.4×10^{-5}	1.3×10^{-4}

TABLE III. The passive approach for the decoy-state BB84 protocol.

	N				
L (km)	10^9	10^{10}	10^{11}	10^{12}	∞
0	2.1×10^{-2}	2.5×10^{-2}	2.8×10^{-2}	3.0×10^{-2}	3.1×10^{-2}
40	1.8×10^{-3}	2.8×10^{-3}	3.6×10^{-3}	3.9×10^{-3}	4.3×10^{-3}
80	8.3×10^{-5}	3.0×10^{-4}	4.4×10^{-4}	5.5×10^{-4}	6.3×10^{-4}
120	0	1.7×10^{-5}	4.6×10^{-5}	7.2×10^{-5}	9.9×10^{-5}
160	0	0	1.6×10^{-6}	5.4×10^{-6}	1.4×10^{-5}

$\epsilon_{\rm cor} \approx \sqrt{\epsilon_{\rm PE}}$ and $\epsilon_{\rm PE} = 11\epsilon$ (rather than 21ϵ) in the active protocol, we take $\epsilon = 2 \times 10^{-20}$ (rather than 10^{-20}) for the overall security to approximately match in both scenarios.

As already pointed out in Refs. [35,36], the drop in the key rate is mainly due to the extra sifting and the higher BER inherent in the passive approach.

IX. CONCLUSIONS AND OUTLOOK

Passive QKD replaces all active modulation in the QKD hardware by a fixed quantum mechanism and postselection, in so doing, benefitting from a considerable simplicity, immunity to modulator side channels, and conceivably higher clock rates. In this work, we have derived finite-key security bounds for a fully passive decoy-state BB84 protocol. For this purpose, we have sharpened the security analysis of Ref. [36] and generalized it to the finite-key regime, considering the postselection strategy originally proposed in Ref. [35]. As a result, the secret-key rate per pulse achievable with our passive scheme is closer than previously reported to the corresponding key rate with an active setup. On top of this, the bounds derived here have been applied to a pioneering fully passive QKD demonstration [37], showing that passive QKD solutions are ready for deployment.

On another note, different avenues could be explored to improve this work. As an example, for moderate numbers of transmission rounds, a slight advantage might be achieved replacing the TD constraints with tighter nonlinear constraints provided by the Cauchy-Schwarz inequality and running semidefinite programs—rather than linear programs—for the parameter estimation (see, e.g., Ref. [14,53]). Interestingly as well, one could attempt to meet existing experimental limitations by relaxing the assumptions on the passive source, say, regarding the perfect visibility interference or the noiseless measurements in Alice’s module.

On the experimental side, efforts should be made to thoroughly understand the potential implementation weaknesses of a fully passive QKD source, together with possible mitigation strategies and countermeasures. In particular, the immunity to modulator side channels comes at the price of integrating a measurement unit in the QKD source for postselection purposes. Naturally, Alice must ensure that the photodetectors in this unit do not emit signals to the channel containing information about the prepared states. In fact, Alice’s measurement unit might be subject to active tampering as well. For instance, Eve could try to sabotage the postselection by injecting external light in the passive source to alter the reading of the detectors. In a similar fashion, a laser-seeding attack [54–56] could modify the phase or the intensity of the laser pulses generated in the passive source, potentially compromising the estimation of the secret-key length. As discussed in Ref. [36], the fact that strong coherent light and classical photodiodes are used in the passive source seems to indicate that incorporating less optical isolation at the output port than in the active case may suffice to counter these problems, by rendering the power of the intrusive light negligible with respect to Alice’s signal pulses. Nevertheless, fully passive QKD is an untested emergent solution and the elaboration of a dedicated and complete risk profile is the secure path to follow.

ACKNOWLEDGMENTS

V.Z. acknowledges fruitful discussions with Guillermo Currás and Álvaro Navarrete. Both V.Z. and M.C. acknowledge support from Cisco Systems Inc., 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, Ministerio de Ciencia e Innovación (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, the European Union’s Horizon Europe framework program under the Marie Skłodowska-Curie Grant No. 101072637 (Project QSI) and the project “Quantum Security Networks Partnership” (QSNP, Grant Agreement No. 101114043).

APPENDIX A: TRACE-DISTANCE ARGUMENT

Let ρ and τ be two density matrices of a quantum system of dimension d. The TD argument states that

$$D(\rho,\tau) = \max_{\hat{O}} \left\{ \mathrm{Tr}\left[\hat{O}(\rho-\tau)\right]\right\}, \tag{A1}$$

where the maximization is taken over all positive operators $\hat{O} \leq I$ [57]. Notably, from the definition of the TD, it follows that $D(\rho,\tau)=\sum_{i=1}^{d}|\lambda_i|$, where the λ_i are the eigenvalues of $\rho-\tau$.

APPENDIX B: MATRIX REPRESENTATION OF THE FOCK STATES

Here, we provide a matrix representation of the Fock states prepared by the passive source, reproducing the approach in Ref. [36] (see that work for more details). Precisely, let

$$\mathcal{B}_n = \left\{ |n-k,k\rangle = \frac{a_{\mathrm{R}}^{\dagger n-k} a_{\mathrm{L}}^{\dagger k}}{\sqrt{(n-k)!k!}} |\mathrm{vac}\rangle \,,\ k=0\ldots n \right\}, \tag{B1}$$

where $a_{\mathrm{R}}^{\dagger}$ ($a_{\mathrm{L}}^{\dagger}$) is the creation operator of the right-handed (left-handed) circular-polarization mode. $\mathcal{B}_n$ is an orthonormal basis of the Hilbert space of n indistinguishable photons distributed across two modes. Given $\mathcal{B}_n$, one can make use of the canonical isomorphism

$$\begin{aligned} &|n,0\rangle \rightarrow [1\,0\ldots 0]^t,\ |n-1,1\rangle \rightarrow [0\,1\ldots 0]^t \ \ldots \\ &|1,n-1\rangle \rightarrow [0\ \ldots\ 1\,0]^t,\ |0,n\rangle \rightarrow [0\ \ldots\ 0\,1]^t \end{aligned} \tag{B2}$$

to obtain the density matrices of the Fock states $\sigma_{j,n}^{\mathrm{key}} = \langle e^{-\mu}\mu^n/n!\,|n\rangle\langle n|_{\theta,\phi}\rangle_{\Omega_j^{\mathrm{key}}}/\langle e^{-\mu}\mu^n/n!\rangle_{\Omega_j^{\mathrm{key}}}$ and $\sigma_{j,n}^{\mathrm{H}} = \langle e^{-\mu}\mu^n/n!\,|n\rangle\langle n|_{\theta,\phi}\rangle_{\Omega_j^{\mathrm{H}}}/\langle e^{-\mu}\mu^n/n!\rangle_{\Omega_j^{\mathrm{H}}}$ (i.e., the ones required for the LPs in the main text) by recalling that

$$|n\rangle_{\theta,\phi} = \frac{1}{\sqrt{n!}}\left[\cos\left(\frac{\theta}{2}\right) a_{\mathrm{R}}^{\dagger} + e^{i\phi}\sin\left(\frac{\theta}{2}\right) a_{\mathrm{L}}^{\dagger}\right]^n |\mathrm{vac}\rangle\,. \tag{B3}$$

For instance, the (r,s)th entry of $\sigma_{j,n}^{\mathrm{key}}$ is computed as $\langle n-r+1,r-1|\,\sigma_{j,n}^{\mathrm{key}}\,|n-s+1,s-1\rangle$ for $r,s=1\ldots n+1$, which in fact vanishes for the off-diagonal terms ($r\neq s$).

APPENDIX C: SECURITY CLAIMS

Definition 1 (correctness).—A pair of keys $(\mathbf{S}_{\mathrm{A}},\mathbf{S}_{\mathrm{B}})$ is ϵ_{cor}-correct if $\Pr[\mathbf{S}_{\mathrm{A}}\neq\mathbf{S}_{\mathrm{B}}]\leq\epsilon_{\mathrm{cor}}$.

Proposition 1 (correctness claim).—The output keys of the protocol are ϵ_{cor}-correct.

Proof.—Let $\perp$ ($\top$) denote the abortion (nonabortion) event. Assuming that the protocol outputs two identical default symbols in case of abortion, i.e., $\Pr[\mathbf{S}_{\mathrm{A}}\neq\mathbf{S}_{\mathrm{B}}\ \wedge\ \perp]=0$, and hence correctness follows if $\Pr[\mathbf{S}_{\mathrm{A}}\neq\mathbf{S}_{\mathrm{B}}\ \wedge\ \top]\leq\epsilon_{\mathrm{cor}}$. Let h_{EV} (h_{PA}) denote the two-universal hash function deployed for EV (PA) and let $\mathbf{K}_{\mathrm{A}}$ ($\mathbf{K}_{\mathrm{B}}$) denote Alice's sifted key (Bob's error-corrected key), such that $\mathbf{S}_{\mathrm{A}}=h_{\mathrm{PA}}(\mathbf{K}_{\mathrm{A}})$ ($\mathbf{S}_{\mathrm{B}}=h_{\mathrm{PA}}(\mathbf{K}_{\mathrm{B}})$). We have

$$\begin{aligned} &\Pr[\mathbf{S}_{\mathrm{A}}\neq\mathbf{S}_{\mathrm{B}}\ \wedge\ \top] \\ &\quad\leq \Pr[h_{\mathrm{PA}}(\mathbf{K}_{\mathrm{A}})\neq h_{\mathrm{PA}}(\mathbf{K}_{\mathrm{B}})\ \wedge\ h_{\mathrm{EV}}(\mathbf{K}_{\mathrm{A}})=h_{\mathrm{EV}}(\mathbf{K}_{\mathrm{B}})] \\ &\quad\leq \Pr[\mathbf{K}_{\mathrm{A}}\neq\mathbf{K}_{\mathrm{B}}\ \wedge\ h_{\mathrm{EV}}(\mathbf{K}_{\mathrm{A}})=h_{\mathrm{EV}}(\mathbf{K}_{\mathrm{B}})] \\ &\quad= \Pr[\mathbf{K}_{\mathrm{A}}\neq\mathbf{K}_{\mathrm{B}}] \\ &\qquad\times\Pr[h_{\mathrm{EV}}(\mathbf{K}_{\mathrm{A}})=h_{\mathrm{EV}}(\mathbf{K}_{\mathrm{B}})\mid\mathbf{K}_{\mathrm{A}}\neq\mathbf{K}_{\mathrm{B}}] \\ &\quad\leq \Pr[h_{\mathrm{EV}}(\mathbf{K}_{\mathrm{A}})=h_{\mathrm{EV}}(\mathbf{K}_{\mathrm{B}})\mid\mathbf{K}_{\mathrm{A}}\neq\mathbf{K}_{\mathrm{B}}]\leq\epsilon_{\mathrm{cor}}. \end{aligned} \tag{C1}$$

The first inequality follows because $\{\top\}\implies\{h_{\mathrm{EV}}(\mathbf{K}_{\mathrm{A}})=h_{\mathrm{EV}}(\mathbf{K}_{\mathrm{B}})\}$, the second inequality follows because $\{h_{\mathrm{PA}}(\mathbf{K}_{\mathrm{A}})\neq h_{\mathrm{PA}}(\mathbf{K}_{\mathrm{B}})\}\implies\{\mathbf{K}_{\mathrm{A}}\neq\mathbf{K}_{\mathrm{B}}\}$, the third inequality follows because $\Pr[\mathbf{K}_{\mathrm{A}}\neq\mathbf{K}_{\mathrm{B}}]\leq 1$, and the fourth inequality follows by the definition of two-universal hashing [47]. ■

Definition 2 (secrecy).—Let $\rho_{\mathrm{SE}}=\sum_{s_{\mathrm{A}}}\Pr[\mathbf{S}_{\mathrm{A}}=s_{\mathrm{A}}]\,|s_{\mathrm{A}}\rangle\langle s_{\mathrm{A}}|_{\mathrm{A}}\otimes\rho_{\mathrm{E}}^{s_{\mathrm{A}}}$ be a bipartite classical-quantum (cq) state describing a classical register A—modeling a RV $\mathbf{S}_{\mathrm{A}}$—and a quantum system E. $\mathbf{S}_{\mathrm{A}}$ is ϵ_{sec}-secret from E if $\min_{\sigma_{\mathrm{E}}} D\left(\rho_{\mathrm{SE}},\omega_{\mathrm{S}}\otimes\sigma_{\mathrm{E}}\right)\leq\epsilon_{\mathrm{sec}}$, where ω_{S} denotes the fully mixed state on A.

Proposition 2 ((secrecy claim)).—Alice's output key in the protocol is $\left(\sqrt{\epsilon_{\mathrm{PE}}}+\epsilon_{\mathrm{PA}}+\delta\right)$-secret from E for

$$l=\left\lfloor M_{\mathrm{key},1}^{\mathrm{L}}\left[1-h\left(e_1^{(\mathrm{ph})\mathrm{U}}\right)\right]-\lambda_{\mathrm{EC}}-\log\left(\frac{1}{2\epsilon_{\mathrm{cor}}\epsilon_{\mathrm{PA}}^2\delta}\right)\right\rfloor, \tag{C2}$$

where $\delta>0$ is arbitrary.

Proof.—The secrecy claim is established here on the basis of the quantum leftover hash lemma [48]. Below, we recast the statement of the lemma provided in Ref. [58].

Theorem 1 ((quantum leftover hash lemma)).—Let $\sigma_{\mathrm{KE}}=\sum_{k_{\mathrm{A}}}\Pr[\mathbf{K}_{\mathrm{A}}=k_{\mathrm{A}}]\,|k_{\mathrm{A}}\rangle\langle k_{\mathrm{A}}|_{\mathrm{A}}\otimes\sigma_{\mathrm{E}}^{k_{\mathrm{A}}}$ be a bipartite cq state and let C be a publicly revealed classical RV. Applying random two-universal hashing on the register A, an $(\epsilon+\epsilon_{\mathrm{PA}})$-secret-from-$E$ key of length

$$l=\left\lfloor H_{\min}^{\epsilon}(\mathbf{K}_{\mathrm{A}}|CE)_{\sigma}-\log\left(\frac{1}{4\epsilon_{\mathrm{PA}}^2}\right)\right\rfloor \tag{C3}$$

can be extracted, where $H_{\min}^{\epsilon}(\mathbf{K}_{\mathrm{A}}|CE)_{\sigma}$ denotes the ϵ-smooth conditional min-entropy of $\mathbf{K}_{\mathrm{A}}$ given access to E and C, evaluated in σ_{KE}.

For our purposes, σ_{KE} is a fully general description of Alice's and Eve's cq state prior to PA, from which the final state $\rho_{\rm SE}$ is obtained in the protocol via random two-universal hashing on the register A. According to Theorem 1, the goal is to derive a lower bound on $H_{\rm min}^{\epsilon}(\mathbf{K}_{\rm A}|CE)_{\sigma}$, which is the purpose of the rest of the proof.

The RV C matches the information revealed by EC and EV in the protocol. Since EC discloses $\lambda_{\rm EC}$ syndrome bits at most and EV discloses $\lceil \log(1/\epsilon_{\rm cor})\rceil < \log(2/\epsilon_{\rm cor})$ EV-tag bits at most, it follows that

$$H_{\rm min}^{\epsilon}(\mathbf{K}_{\rm A}|CE)_{\sigma} \geq H_{\rm min}^{\epsilon}(\mathbf{K}_{\rm A}|E)_{\sigma} - \lambda_{\rm EC} - \log\left(\frac{2}{\epsilon_{\rm cor}}\right), \tag{C4}$$

by applying a chain rule for smooth min-entropies [58]. Next, we decompose the RV $\mathbf{K}_{\rm A}$ as $\mathbf{K}_{\rm A} = \mathbf{K}_{\rm A}^{1}\mathbf{K}_{\rm A}^{\rm rest}$, where $\mathbf{K}_{\rm A}^{1}$ describes those sifted key bits corresponding to single-photon-detection events and $\mathbf{K}_{\rm A}^{\rm rest}$ describes the rest of the bits. From this decomposition and a generalized chain rule given in Ref. [59], it follows that

$$H_{\rm min}^{\epsilon}(\mathbf{K}_{\rm A}|E)_{\sigma} \geq H_{\rm min}^{\epsilon-\delta}(\mathbf{K}_{\rm A}^{1}|E)_{\sigma} - \log\left(\frac{1}{\delta}\right), \tag{C5}$$

for all $\delta \in (0,\epsilon)$, and plugging Eq. (C5) into Eq. (C4) yields

$$H_{\rm min}^{\epsilon}(\mathbf{K}_{\rm A}|CE)_{\sigma} \geq H_{\rm min}^{\epsilon-\delta}(\mathbf{K}_{\rm A}^{1}|E)_{\sigma} - \lambda_{\rm EC} - \log\left(\frac{2}{\epsilon_{\rm cor}\delta}\right). \tag{C6}$$

Thus, all that remains is to lower bound the term $H_{\rm min}^{\epsilon-\delta}(\mathbf{K}_{\rm A}^{1}|E)_{\sigma}$. For this purpose, we make use of the entropic uncertainty relation [60], which we present below in the restricted case of projective measurements (that suffice for our analysis).

Theorem 2 ((entropic uncertainty relation)).—Let $\tau_{\rm ABE}$ be a tripartite quantum state and let key $= \{|k\rangle\,\langle k|_{\rm A}\}$ and test $= \{|t\rangle\,\langle t|_{\rm A}\}$ be two projective measurements on A, $\mathbf{K}$ and $\mathbf{T}$ denoting the RVs associated with their measurement outcomes. Then, for all $\varepsilon \geq 0$,

$$H_{\rm min}^{\varepsilon}(\mathbf{K}|E)_{\tau} + H_{\rm max}^{\varepsilon}(\mathbf{T}|B)_{\tau} \geq q, \tag{C7}$$

where $H_{\rm min}^{\varepsilon}(\mathbf{K}|E)_{\tau}$ denotes the ϵ-smooth conditional min-entropy of $\mathbf{K}$ given E evaluated in the bipartite cq state $\tau_{\rm KE} = \sum_{k}{\rm Pr}[\mathbf{K}=k]\,|k\rangle\,\langle k|_{\rm A} \otimes \tau_{\rm E}^{k}$, $H_{\rm max}^{\varepsilon}(\mathbf{T}|B)_{\tau}$ denotes the ϵ-smooth conditional max-entropy of $\mathbf{T}$ given B evaluated in the bipartite cq state $\tau_{\rm TB} = \sum_{t}{\rm Pr}[\mathbf{T}=t]\,|t\rangle\,\langle t|_{\rm A} \otimes \tau_{\rm B}^{t}$, and $q = \log\frac{1}{c}$ for $c = \max_{k,t}|\langle k|t\rangle|^{2}$.

Let $\tau_{\rm ABE}^{1}$ be the classical-quantum-quantum state describing:

(1) The subregister $\rm A^{1}$ of A that models the RV $\mathbf{K}_{\rm A}^{1}$ ($\mathbf{T}_{\rm A}^{1}$) via a projective measurement key (test) in the key basis (test basis).

(2) Bob's quantum side information on $\rm A^{1}$, say $\rm B^{1}$.

(3) Eve's quantum side information on $\rm A^{1}$, say $\rm E^{1}$.

Crucially, this choice of $\tau_{\rm ABE}^{1}$ is such that $\sigma_{\rm KE}$ provides an extension of $\tau_{\rm KE}^{1} = \sum_{k_{\rm A}^{1}}{\rm Pr}\big[\mathbf{K}_{\rm A}^{1} = k_{\rm A}^{1}\big]\,\big|k_{\rm A}^{1}\big\rangle\big\langle k_{\rm A}^{1}\big|_{\rm A} \otimes \tau_{\rm E}^{k_{\rm A}^{1}}$, as the former is related to the latter by suitable partial tracing. This will be relevant to link the entropies of both states.

Also, we have that key $= \big\{\big|k_{\rm A}^{1}\big\rangle\big\langle k_{\rm A}^{1}\big|\big\}$ and test $= \big\{\big|t_{\rm A}^{1}\big\rangle\big\langle t_{\rm A}^{1}\big|\big\}$ for $k_{\rm A}^{1} \in \{{\rm R},{\rm L}\}^{M_{\rm key,1}}$ and $t_{\rm A}^{1} \in \{{\rm H},{\rm V}\}^{M_{\rm key,1}}$, where $M_{\rm key,1}$ denotes the number of bits in the register $\rm A^{1}$ (i.e., the size of $\mathbf{K}_{\rm A}^{1}$). It then follows that $c = \max_{k,t}|\big\langle k_{\rm A}^{1}\big|t_{\rm A}^{1}\big\rangle|^{2} = 2^{-M_{\rm key,1}}$, and by virtue of Theorem 2 we have that

$$H_{\rm min}^{\varepsilon}(\mathbf{K}_{\rm A}^{1}|E^{1})_{\tau^{1}} \geq M_{\rm key,1} - H_{\rm max}^{\varepsilon}(\mathbf{T}_{\rm A}^{1}|B^{1})_{\tau^{1}}. \tag{C8}$$

Equation (C8) sets a fundamental trade-off between Eve's and Bob's predictive powers on the outcomes of mutually unbiased measurements key and test performed on $\rm A^{1}$. Importantly, this trade-off is established *a priori* of any protocol execution.

Similarly, the PE procedure explained in Sec. VII also provides an *a priori* statistical constraint on the RVs $M_{\rm key,1}$ and $m_{\rm key,1}^{\rm (ph)}$ on $\tau_{\rm ABE}^{1}$; namely, that the event

$$\omega = \left\{M_{\rm key,1} \notin \left(M_{\rm key,1}^{\rm L}, M_{\rm key,1}^{\rm U}\right) \cup\, m_{\rm key,1}^{\rm (ph)} \geq m_{\rm key,1}^{{\rm (ph)}\,U}\right\} \tag{C9}$$

(where the bounding RVs $M_{\rm key,1}^{\rm L}$, $M_{\rm key,1}^{\rm U}$ and $m_{\rm key,1}^{{\rm (ph)}\,U}$ are defined in Sec. VII) satisfies ${\rm Pr}[\omega] \leq \epsilon_{\rm PE}$. This result allows one to lower bound $H_{\rm min}^{\varepsilon}(\mathbf{K}_{\rm A}^{1}|E^{1})_{\tau^{1}}$ for a suitably chosen ε using the following lemma [61].

Lemma 1.—Let ρ be a quantum state and let ω be an arbitrary event. If ρ is such that ${\rm Pr}[\omega] \leq \epsilon$, there exists another state $\tilde{\rho}$, $\sqrt{\epsilon}$-close to ρ in purified distance, i.e., verifying $P(\rho,\tilde{\rho}) \leq \sqrt{\epsilon}$, for which ${\rm Pr}[\omega] = 0$.

By virtue of Lemma 1 (for a definition of the purified distance, see Ref. [61]), there exists a quantum state $\tilde{\tau}_{\rm ABE}^{1}$ with $P(\tau_{\rm ABE}^{1}, \tilde{\tau}_{\rm ABE}^{1}) \leq \sqrt{\epsilon_{\rm PE}}$ for which ${\rm Pr}[\omega] = 0$. In what follows, we use this state as an artifact to lower bound $H_{\rm min}^{\sqrt{\epsilon_{\rm PE}}}(\mathbf{K}_{\rm A}^{1}|E^{1})_{\tau^{1}}$.

First, particularizing Eq. (C8) for $\tilde{\tau}_{\rm ABE}^{1}$ in the limit case $\varepsilon = 0$, we have that

$$H_{\rm min}(\mathbf{K}_{\rm A}^{1}|E^{1})_{\tilde{\tau}^{1}} \geq M_{\rm key,1} - H_{\rm max}(\mathbf{T}_{\rm A}^{1}|B^{1})_{\tilde{\tau}^{1}}. \tag{C10}$$

Next, we will derive an upper bound on the nonsmooth max-entropy $H_{\rm max}(\mathbf{T}_{\rm A}^{1}|B^{1})_{\tilde{\tau}^{1}}$. For this purpose, let us consider the set of quantum signals that contribute to $\mathbf{K}_{\rm A}^{1}$. In particular, let $\mathbf{T}_{\rm B}^{1}$ be the RV defined by the outcome of measuring this set of signals in the test basis. Clearly, $H_{\rm max}(\mathbf{T}_{\rm A}^{1}|B^{1})_{\tilde{\tau}^{1}} \leq H_{\rm max}(\mathbf{T}_{\rm A}^{1}|\mathbf{T}_{\rm B}^{1})_{\tilde{\tau}^{1}}$ because $\mathbf{T}_{\rm B}^{1}$ is accessible given B^{1}. Moreover, $H_{\rm max}(\mathbf{T}_{\rm A}^{1}|\mathbf{T}_{\rm B}^{1})_{\tilde{\tau}^{1}}$ is quantified by the logarithm of the number of outcomes for $\mathbf{T}_{\mathrm{A}}^{1}$ with a nonzero probability to occur. Precisely [61],

$$H_{\max}(\mathbf{T}_{\mathrm{A}}^{1}|\mathbf{T}_{\mathrm{B}}^{1})_{\tilde{\tau}} \leq \max_{t_{\mathrm{B}}^{1}:\Pr\left[\mathbf{T}_{\mathrm{B}}^{1}=t_{\mathrm{B}}^{1}\right]>0} \log\left|\left\{t_{\mathrm{A}}^{1}\ :\ \Pr\left[\mathbf{T}_{\mathrm{A}}^{1}=t_{\mathrm{A}}^{1}|\mathbf{T}_{\mathrm{B}}^{1}=t_{\mathrm{B}}^{1}\right]>0\right\}\right|, \tag{C11}$$

and given an upper bound $e_{1}^{(\mathrm{ph})\,\mathrm{U}}$ on the ratio of errors $e_{1}^{(\mathrm{ph})}$ between $\mathbf{T}_{\mathrm{A}}^{1}$ and $\mathbf{T}_{\mathrm{B}}^{1}$—namely, the so-called phase-error rate—this can be upper bounded via [62]

$$H_{\max}(\mathbf{T}_{\mathrm{A}}^{1}|\mathbf{T}_{\mathrm{B}}^{1})_{\tilde{\tau}} \leq M_{\mathrm{key},1}\, h\left(e_{1}^{(\mathrm{ph})\,\mathrm{U}}\right), \tag{C12}$$

where $h(x)$ is the binary entropy function. Plugging this into Eq. (C10) we obtain

$$H_{\min}(\mathbf{K}_{\mathrm{A}}^{1}|E^{1})_{\tilde{\tau}^{1}} \geq M_{\mathrm{key},1}\left[1-h\left(e_{1}^{(\mathrm{ph})\,\mathrm{U}}\right)\right]. \tag{C13}$$

Crucially, for $\tilde{\tau}_{\mathrm{ABE}}^{1}$, $M_{\mathrm{key},1}$ and $e_{1}^{(\mathrm{ph})\,\mathrm{U}}$ can be related to observables of the protocol because of the fact that $\Pr[\omega]=0$. On the one hand, the latter implies that $M_{\mathrm{key},1} \in \left(M_{\mathrm{key},1}^{\mathrm{L}}, M_{\mathrm{key},1}^{\mathrm{U}}\right)$. On the other, it implies that $m_{\mathrm{key},1}^{(\mathrm{ph})} \leq m_{\mathrm{key},1}^{(\mathrm{ph})\,U}$, such that one can choose

$$e_{1}^{(\mathrm{ph})\,\mathrm{U}} = \min\left\{\frac{m_{\mathrm{key},1}^{(\mathrm{ph})\,\mathrm{U}}}{M_{\mathrm{key},1}^{\mathrm{L}}}, \frac{1}{2}\right\}, \tag{C14}$$

for $\tilde{\tau}_{\mathrm{ABE}}^{1}$. As a consequence, it follows that

$$H_{\min}(\mathbf{K}_{\mathrm{A}}^{1}|E^{1})_{\tilde{\tau}^{1}} \geq M_{\mathrm{key},1}^{\mathrm{L}}\left[1-h\left(e_{1}^{(\mathrm{ph})\,\mathrm{U}}\right)\right]. \tag{C15}$$

Now, since $H_{\min}^{\varepsilon}(\mathbf{X}|Y)_{\rho} = \max_{P(\rho,\tilde{\rho})\,\leq\,\varepsilon} H_{\min}(\mathbf{X}|Y)_{\tilde{\rho}}$, it follows from Eq. (C15) that $H_{\min}^{\sqrt{\epsilon_{\mathrm{PE}}}}(\mathbf{K}_{\mathrm{A}}^{1}|E^{1})_{\tau^{1}} \geq M_{\mathrm{key},1}^{\mathrm{L}}\big[1-h\big(e_{1}^{(\mathrm{ph})\,\mathrm{U}}\big)\big]$ by noting that $P(\tau_{\mathrm{KE}}^{1},\tilde{\tau}_{\mathrm{KE}}^{1}) \leq P(\tau_{\mathrm{ABE}}^{1}, \tilde{\tau}_{\mathrm{ABE}}^{1}) \leq \sqrt{\epsilon_{\mathrm{PE}}}$ (in the penultimate inequality, we are using the fact that the purified distance is nonincreasing under trace nonincreasing completely positive maps [63]).

In fact, the exact same bound holds for $H_{\min}^{\sqrt{\epsilon_{\mathrm{PE}}}}(\mathbf{K}_{\mathrm{A}}^{1}|E)_{\sigma}$ directly—and not just for $H_{\min}^{\sqrt{\epsilon_{\mathrm{PE}}}}(\mathbf{K}_{\mathrm{A}}^{1}|E^{1})_{\tau^{1}}$—by virtue of the following lemma [64].

Lemma 2.—For any two states τ and $\tilde{\tau}$ and any extension σ of τ, there exists an extension $\tilde{\sigma}$ with $P(\sigma,\tilde{\sigma}) = P(\tau,\tilde{\tau})$.

In particular, since σ_{KE} is an extension of τ_{KE}^{1} and $P(\tau_{\mathrm{KE}}^{1},\tilde{\tau}_{\mathrm{KE}}^{1}) \leq \sqrt{\epsilon_{\mathrm{PE}}}$, there exists an extension $\tilde{\sigma}_{\mathrm{KE}}$ of $\tilde{\tau}_{\mathrm{KE}}^{1}$ such that $P(\sigma_{\mathrm{KE}},\tilde{\sigma}_{\mathrm{KE}}) \leq \sqrt{\epsilon_{\mathrm{PE}}}$, meaning that $H_{\min}^{\sqrt{\epsilon_{\mathrm{PE}}}}(\mathbf{K}_{\mathrm{A}}^{1}|E)_{\sigma} \geq H_{\min}(\mathbf{K}_{\mathrm{A}}^{1}|E)_{\tilde{\sigma}}$. What is more, let $p_{\mathrm{guess}}(\mathbf{X}|Y)_{\rho}$ denote the probability of guessing $\mathbf{X}$ given access to Y in an underlying quantum state ρ. As any other extension of $\tilde{\tau}_{\mathrm{KE}}^{1}$, $\tilde{\sigma}_{\mathrm{KE}}$ verifies $p_{\mathrm{guess}}(\mathbf{K}_{\mathrm{A}}^{1}|E)_{\tilde{\sigma}} = p_{\mathrm{guess}}(\mathbf{K}_{\mathrm{A}}^{1}|E^{1})_{\tilde{\tau}^{1}}$ by the *ad hoc* definition of E^{1}—according to which E^{1} is the share of E correlated to A^{1} within the underlying state. Therefore, $H_{\min}(\mathbf{K}_{\mathrm{A}}^{1}|E)_{\tilde{\sigma}} = H_{\min}(\mathbf{K}_{\mathrm{A}}^{1}|E^{1})_{\tilde{\tau}^{1}}$ by definition of the nonsmooth min-entropy [61].

In summary, the extension $\tilde{\sigma}_{\mathrm{KE}}$ provided by Lemma 2 allows one to establish that

$$\begin{aligned} H_{\min}^{\sqrt{\epsilon_{\mathrm{PE}}}}(\mathbf{K}_{\mathrm{A}}^{1}|E)_{\sigma} &\geq H_{\min}(\mathbf{K}_{\mathrm{A}}^{1}|E)_{\tilde{\sigma}} = H_{\min}(\mathbf{K}_{\mathrm{A}}|E^{1})_{\tilde{\tau}^{1}} \\ &\geq M_{\mathrm{key},1}^{\mathrm{L}}\left[1-h\left(e_{1}^{(\mathrm{ph})\,\mathrm{U}}\right)\right], \end{aligned} \tag{C16}$$

where the last inequality follows from Eq. (C15). According to Eq. (C6), this bound on $H_{\min}^{\sqrt{\epsilon_{\mathrm{PE}}}}(\mathbf{K}_{\mathrm{A}}^{1}|E)_{\sigma}$ implies the bound

$$\begin{aligned} H_{\min}^{\sqrt{\epsilon_{\mathrm{PE}}}+\delta}(\mathbf{K}_{\mathrm{A}}|CE)_{\sigma} &\geq M_{\mathrm{key},1}^{\mathrm{L}}\left[1-h\left(e_{1}^{(\mathrm{ph})\,\mathrm{U}}\right)\right] \\ &- \lambda_{\mathrm{EC}} - \log\left(\frac{2}{\epsilon_{\mathrm{cor}}\delta}\right), \end{aligned} \tag{C17}$$

for all $\delta > 0$. Lastly, since ρ_{SE} is obtained in the protocol by applying random two-universal hashing on the register A of σ_{KE}, the secrecy claim follows from Theorem 1. ■

APPENDIX D: KATO'S INEQUALITY

Let $\xi_{1},\xi_{2}\ldots\xi_{N}$ be a sequence of Bernoulli RVs and let $\mathcal{F}_{0}\subseteq\mathcal{F}_{1}\subseteq\ldots\subseteq\mathcal{F}_{N}$ be an increasing chain of σ-algebras verifying $E\left(\xi_{v}|\mathcal{F}_{u}\right)=\xi_{v}$ for $v\leq u$. Kato's inequality [44] states that

$$\Pr\left[\sum_{u=1}^{N}\Pr\left(\xi_{u}=1|\mathcal{F}_{u-1}\right)-\Lambda_{N}\geq\left[b+a\left(\frac{2\Lambda_{N}}{N}-1\right)\right]\sqrt{N}\right]\leq\exp\left[\frac{-2(b^{2}-a^{2})}{\left(1+\frac{4a}{3\sqrt{N}}\right)^{2}}\right], \tag{D1}$$

for any $N \in \mathbb{N}$, $a \in \mathbb{R}$ and $b \in \mathbb{R}^+$ such that $b > |a|$, where we have defined $\Lambda_l = \sum_{u=1}^{l} \xi_u$. Moreover, replacing ξ_l by $1 - \xi_l$ and a by $-a$ in Eq. (D1), it trivially follows that

$$\Pr\left[\Lambda_N - \sum_{u=1}^{N} \Pr\left(\xi_u = 1|\mathcal{F}_{u-1}\right) \geq \left[b + a\left(\frac{2\Lambda_N}{N} - 1\right)\right]\sqrt{N}\right] \leq \exp\left[\frac{-2(b^2 - a^2)}{\left(1 - \frac{4a}{3\sqrt{N}}\right)^2}\right]. \tag{D2}$$

1. Direct Kato bounds

Equation (D2) provides a family of lower bounds on $\sum_{u=1}^{N} \Pr\left(\xi_u = 1|\mathcal{F}_{u-1}\right)$ given Λ_N and we want to reach the tightest possible bound compatible with a certain error probability ϵ. Hence, among all pairs (a, b) that fulfill the ϵ error-probability condition, we must pick the one that minimizes the deviation term. However, since the latter depends on the realization Λ_N, this task requires us to come up with a preliminary guess, say, $\tilde{\Lambda}_N$, of Λ_N, with respect to which the minimization can be carried out. In short, the problem to address is

$$\begin{aligned} &\arg\min_{a,b} \quad \left[b + a\left(\frac{2\tilde{\Lambda}_N}{N} - 1\right)\right]\sqrt{N} \\ &\text{such that} \quad \exp\left[\frac{-2(b^2 - a^2)}{\left(1 - \frac{4a}{3\sqrt{N}}\right)^2}\right] = \epsilon, \quad b \geq |a|. \end{aligned} \tag{D3}$$

Its solution is [65]

$$\begin{aligned} a &= \frac{3\left\{9\sqrt{2}N\left(N - 2\tilde{\Lambda}_N\right)\sqrt{-\ln\epsilon\left[9\tilde{\Lambda}_N\left(N - \tilde{\Lambda}_N\right) - 2N\ln\epsilon\right]} + 16N^{3/2}\ln^2\epsilon - 72\tilde{\Lambda}_N\sqrt{N}\left(N - \tilde{\Lambda}_N\right)\ln\epsilon\right\}}{4\left(9N - 8\ln\epsilon\right)\left[9\tilde{\Lambda}_N\left(N - \tilde{\Lambda}_N\right) - 2N\ln\epsilon\right]}, \\ b &= \frac{\sqrt{18Na^2 - \left(16a^2 - 24\sqrt{N}a + 9N\right)\ln\epsilon}}{3\sqrt{2N}}, \end{aligned} \tag{D4}$$

leading to the bound

$$\sum_{u=1}^{N} \Pr\left(\xi_u = 1|\mathcal{F}_{u-1}\right) \overset{\epsilon}{>} K^{\mathrm{L}}_{N,\epsilon}\left(\Lambda_N\right), \tag{D5}$$

for $K^{\mathrm{L}}_{N,\epsilon}\left(\Lambda_N\right) = \Lambda_N - \left[b + a\left(2\Lambda_N/N - 1\right)\right]\sqrt{N}$. Of course, the closer Λ_N happens to be from $\tilde{\Lambda}_N$, the tighter the bound becomes, but it holds true in any case.

Analogously, one can tune a and b in Eq. (D1) to reach the tightest possible upper bound on $\sum_{u=1}^{N} \Pr\left(\xi_u = 1|\mathcal{F}_{u-1}\right)$ compatible with a fixed error probability ϵ, should the guess $\tilde{\Lambda}_N$ become true. The corresponding problem is

$$\begin{aligned} &\arg\min_{a,b} \quad \left[b + a\left(\frac{2\tilde{\Lambda}_N}{N} - 1\right)\right]\sqrt{N} \\ &\text{such that} \quad \exp\left[\frac{-2(b^2 - a^2)}{\left(1 + \frac{4a}{3\sqrt{N}}\right)^2}\right] = \epsilon, \quad b \geq |a|. \end{aligned} \tag{D6}$$

Its solution is [65]

$$a=\frac{3\left\{9\sqrt{2}N\left(N-2\tilde{\Lambda}_N\right)\sqrt{-\ln\epsilon\left[9\tilde{\Lambda}_N\left(N-\tilde{\Lambda}_N\right)-2N\ln\epsilon\right]}-16N^{3/2}\ln^2\epsilon+72\tilde{\Lambda}_N\sqrt{N}\left(N-\tilde{\Lambda}_N\right)\ln\epsilon\right\}}{4\left(9N-8\ln\epsilon\right)\left[9\tilde{\Lambda}_N\left(N-\tilde{\Lambda}_N\right)-2N\ln\epsilon\right]},$$
$$b=\frac{\sqrt{18Na^2-\left(16a^2+24\sqrt{N}a+9N\right)\ln\epsilon}}{3\sqrt{2N}}, \tag{D7}$$

leading to the bound

$$\sum_{u=1}^{N}\Pr\left(\xi_u=1|\mathcal{F}_{u-1}\right)\overset{\epsilon}{<}K^{\mathrm{U}}_{N,\epsilon}\left(\Lambda_N\right) \tag{D8}$$

for $K^{\mathrm{U}}_{N,\epsilon}\left(\Lambda_N\right)=\Lambda_N+\left[b+a\left(2\Lambda_N/N-1\right)\right]\sqrt{N}$.

2. Reverse Kato bounds

Similar arguments allow one to bound Λ_N given $S_N=\sum_{u=1}^{N}\Pr\left(\xi_u=1|\mathcal{F}_{u-1}\right)$, based on a preliminary guess $\tilde{S}_N$ of the latter to pick suitable values of a and b.

On the one hand, from Eq. (D1) one can readily show that $\Lambda_N\overset{\epsilon}{>}\bar{K}^{\mathrm{L}}_{N,\epsilon}\left(S_N\right)$ for $\bar{K}^{\mathrm{L}}_{N,\epsilon}\left(S_N\right)=\left[\sqrt{N}S_N+N(a-b)\right]/(2a+\sqrt{N})$, where (a,b) is the solution to

$$\begin{aligned}&\underset{a,b}{\arg\max}\quad\frac{\sqrt{N}\tilde{S}_N+N(a-b)}{2a+\sqrt{N}}\\&\text{such that}\quad\exp\left[\frac{-2(b^2-a^2)}{\left(1+\dfrac{4a}{3\sqrt{N}}\right)^2}\right]=\epsilon,\quad b\geq|a|,\end{aligned} \tag{D9}$$

given by [24]

$$a=\frac{3\sqrt{N}\left\{9\left(N-2\tilde{S}_N\right)\sqrt{N\ln\epsilon\left[N\ln\epsilon-18\tilde{S}_N\left(N-\tilde{S}_N\right)\right]}-4N\ln^2\epsilon-9\left(8\tilde{S}_N^2-8N\tilde{S}_N+3N^2\right)\ln\epsilon\right\}}{4\left\{4N\ln^2\epsilon+36\left(2\tilde{S}_N^2-2N\tilde{S}_N+N^2\right)\ln\epsilon+81N\tilde{S}_N\left(N-\tilde{S}_N\right)\right\}},$$
$$b=\frac{1}{3}\sqrt{9a^2-\frac{\left(4a+3\sqrt{N}\right)^2\ln\epsilon}{2N}}. \tag{D10}$$

On the other hand, from Eq. (D2) one can show that $\Lambda_N\overset{\epsilon}{<}\bar{K}^{\mathrm{U}}_{N,\epsilon}\left(S_N\right)$ for $\bar{K}^{\mathrm{U}}_{N,\epsilon}\left(S_N\right)=\left[\sqrt{N}S_N-N(a-b)\right]/(\sqrt{N}-2a)$, where (a,b) is the solution to

$$\begin{aligned}&\underset{a,b}{\arg\min}\quad\frac{\sqrt{N}\tilde{S}_N-N(a-b)}{\sqrt{N}-2a}\\&\text{such that}\quad\exp\left[\frac{-2(b^2-a^2)}{\left(1-\dfrac{4a}{3\sqrt{N}}\right)^2}\right]=\epsilon,\quad b\geq|a|,\end{aligned} \tag{D11}$$

given by [24]

$$
\begin{aligned}
a &= \frac{3\sqrt{N}\left\{9\left(N-2\tilde{S}_N\right)\sqrt{N\ln\epsilon\left[N\ln\epsilon+18\tilde{S}_N\left(\tilde{S}_N-N\right)\right]}+4N\ln^2\epsilon+9\left(8\tilde{S}_N^2-8N\tilde{S}_N+3N^2\right)\ln\epsilon\right\}}{4\left\{4N\ln^2\epsilon+36\left(2\tilde{S}_N^2-2N\tilde{S}_N+N^2\right)\ln\epsilon+81N\tilde{S}_N\left(N-\tilde{S}_N\right)\right\}},\\
b &= \frac{\sqrt{18Na^2-\left(16a^2-24\sqrt{N}a+9N\right)\ln\epsilon}}{3\sqrt{2N}}.
\end{aligned}
\tag{D12}
$$

Finally, let us point out a minor technical issue. Although we have established that $\Lambda_N \overset{\epsilon}{>} \bar{K}^{\mathrm{L}}_{N,\epsilon}\left(S_N\right)$ $(\Lambda_N \overset{\epsilon}{<} \bar{K}^{\mathrm{U}}_{N,\epsilon}\left(S_N\right))$, if only a lower (upper) bound on S_N were known—say, S_N^{L} (S_N^{U})—it would be of interest to guarantee that $\Lambda_N \overset{\epsilon}{>} \bar{K}^{\mathrm{L}}_{N,\epsilon}\left(S_N^{\mathrm{L}}\right)$ $(\Lambda_N \overset{\epsilon}{<} \bar{K}^{\mathrm{U}}_{N,\epsilon}\left(S_N^{\mathrm{U}}\right))$. In fact, this is indeed the case as long as $\bar{K}^{\mathrm{L}}_{N,\epsilon}(x)$ $(\bar{K}^{\mathrm{U}}_{N,\epsilon}(x))$ is a nondecreasing function, which corresponds to the regime $a \geq -\sqrt{N}/2$ $(a \leq \sqrt{N}/2)$. Namely, the desired inequalities hold if we replace a in Eq. (D10) [Eq. (D12)] by $a' = \max\left\{a, -\sqrt{N}/2\right\}$ $\left(a' = \min\left\{a, \sqrt{N}/2\right\}\right)$.

APPENDIX E: USE CASE FOR KATO'S INEQUALITY

To exemplify the application of Kato's inequality [44], below we show that

$$
Nq_{\mathrm{key}}\left\langle 1\right\rangle_{\Omega_j^{\mathrm{key}}} Q_j^{\mathrm{key}} \overset{\epsilon}{>} K^{\mathrm{L}}_{N,\epsilon}(M_j^{\mathrm{key}})
\tag{E1}
$$

within the adversary model presented in Sec. II [note that Eq. (E1) is just one of the multiple usages of Kato's inequality in the main text].

For this purpose, let

$$
\xi_u = \begin{cases} 1, & \text{if Alice postselects } \sigma_{\mathrm{j}}^{\mathrm{key}}\text{, Bob picks the key basis and a “click" occurs in round u,} \\ 0, & \text{otherwise,} \end{cases}
\tag{E2}
$$

for $u = 1, 2 \ldots N$ (such that $\sum_{u=1}^{N} \xi_u = M_j^{\mathrm{key}}$), and let $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \ldots \subseteq \mathcal{F}_N$ be the chain of σ algebras induced by the sequence R_0, (ξ_1, R_1), (ξ_2, R_2), $\ldots$, (ξ_N, R_N). Here, we recall that R_u denotes the state of Eve's classical register at the end of round u and R_0 denotes an arbitrary initial state of the register (see Sec. II). From the definitions of ξ_u and $\mathcal{F}_u$, the condition $E\left(\xi_v|\mathcal{F}_u\right) = \xi_v$ follows for all $v \leq u$ and therefore Kato's inequality applies. Hence, from Eq. (D5) we have that $\sum_{u=1}^{N} \Pr\left(\xi_u = 1|\mathcal{F}_{u-1}\right) \overset{\epsilon}{>} K^{\mathrm{L}}_{N,\epsilon}\left(M_j^{\mathrm{key}}\right)$, such that the desired claim—Eq. (E1)—holds if

$$
\sum_{u=1}^{N} \Pr\left(\xi_u = 1|\mathcal{F}_{u-1}\right) = Nq_{\mathrm{key}}\left\langle 1\right\rangle_{\Omega_j^{\mathrm{key}}} Q_j^{\mathrm{key}}.
\tag{E3}
$$

This is what we establish next. On the one hand, by definition of Q_j^{key}, the right-hand side of Eq. (E3) can be written as $\sum_{u=1}^{N} q_{\mathrm{key}}\left\langle 1\right\rangle_{\Omega_j^{\mathrm{key}}} p^{(u)}\left(\mathrm{click}|R_{u-1}, \sigma_j^{\mathrm{key}}, \mathrm{key}\right)$. As for the l.h.s., we have $\Pr\left(\xi_u = 1|\mathcal{F}_{u-1}\right) = p^{(u)}\left(\sigma_j^{\mathrm{key}}, \mathrm{key}, \mathrm{click}|\mathcal{F}_{u-1}\right) = q_{\mathrm{key}}\left\langle 1\right\rangle_{\Omega_j^{\mathrm{key}}} p^{(u)}\left(\mathrm{click}|\mathcal{F}_{u-1}, \sigma_j^{\mathrm{key}}, \mathrm{key}\right)$, simply using the definition of ξ_u and the fact that $p^{(u)}\left(\sigma_j^{\mathrm{key}}, \mathrm{key}|\mathcal{F}_{u-1}\right) = q_{\mathrm{key}}\left\langle 1\right\rangle_{\Omega_j^{\mathrm{key}}}$. In short, Eq. (E3) follows if

$$
p^{(u)}\left(\mathrm{click}|\mathcal{F}_{u-1}, \sigma_j^{\mathrm{key}}, \mathrm{key}\right) = p^{(u)}\left(\mathrm{click}|R_{u-1}, \sigma_j^{\mathrm{key}}, \mathrm{key}\right).
\tag{E4}
$$

Remarkably though, this condition is true by hypothesis in our adversary model, since by assumption the only influence $\mathcal{F}_{u-1}$ may have on round u is captivated by R_{u-1}.

APPENDIX F: CHANNEL MODEL

For the simulations of Sec. VIII, the protocol observables are set to their expected values according to a standard channel model thoroughly described in Ref. [36]. For simplicity, the model disregards any possible misalignment occurring in the QKD link and an active QKD receiver is assumed for comparison with prior work.

Given the overall efficiency of the system, η (accounting for both channel and detection losses), and the dark-count probability of Bob's detectors, p_{d}, for all possible intensity settings j the model yields

$$\mathbb{E}\left[M_j^{\mathrm{key}}\right] = Nq_{\mathrm{key}}\left\langle 1-(1-p_{\mathrm{d}})^2 e^{-I\eta}\right\rangle_{\Omega_j^{\mathrm{key}}}, \quad \mathbb{E}\left[M_j^{\mathrm{test}}\right] = Nq_{\mathrm{test}}\left\langle 1-(1-p_{\mathrm{d}})^2 e^{-I\eta}\right\rangle_{\Omega_j^{\mathrm{test}}} \tag{F1}$$

for the numbers of counts and

$$\mathbb{E}\left[m_j^{\mathrm{test}}\right] = 2\times Nq_{\mathrm{test}}\left\langle \frac{1}{2}\left[1-(1-p_{\mathrm{d}})^2 e^{-I\eta}\right] - \frac{1}{2}(1-p_{\mathrm{d}})\left[e^{-\frac{I\eta(1-\sin\theta\cos\phi)}{2}} - e^{-\frac{I\eta(1+\sin\theta\cos\phi)}{2}}\right]\right\rangle_{\Omega_j^{\mathrm{H}}} \tag{F2}$$

for the numbers of test-basis error counts. In a similar fashion, the size of the sifted keys, $M_{\mathrm{key}} = |\mathcal{X}^{\mathrm{key}}|$, and the corresponding number of bit errors—say, m_{key}—obey

$$\mathbb{E}\left[M_{\mathrm{key}}\right] = Nq_{\mathrm{key}}\left\langle 1-(1-p_{\mathrm{d}})^2 e^{-I\eta}\right\rangle_{\Omega^{\mathrm{key}}} \tag{F3}$$

and

$$\mathbb{E}\left[m_{\mathrm{key}}\right] = 2\times Nq_{\mathrm{key}}\left\langle \frac{1}{2}\left[1-(1-p_{\mathrm{d}})^2 e^{-I\eta}\right] - \frac{1}{2}(1-p_{\mathrm{d}})\left[e^{-I\eta\sin^2\frac{\theta}{2}} - e^{-I\eta\cos^2\frac{\theta}{2}}\right]\right\rangle_{\Omega^{\mathrm{R}}}, \tag{F4}$$

where we recall that $\Omega^{\mathrm{key}} = \bigcup_{j\in\Gamma^{\mathrm{key}}}\Omega_j^{\mathrm{key}}$ and we have also introduced $\Omega^{\mathrm{R}} = \bigcup_{j\in\Gamma^{\mathrm{key}}}\Omega_j^{\mathrm{R}}$ [note that Eq. (F4) explicitly uses the fact that both polar caps contribute equally to the bit errors within the channel model]. Importantly, $\mathbb{E}\left[M_{\mathrm{key}}\right]$ and $\mathbb{E}\left[m_{\mathrm{key}}\right]$ determine the model that we use for the error-correction leakage in the simulations via

$$\lambda_{\mathrm{EC}} = f_{\mathrm{EC}}\mathbb{E}\left[M_{\mathrm{key}}\right] h\left(\frac{\mathbb{E}\left[m_{\mathrm{key}}\right]}{\mathbb{E}\left[M_{\mathrm{key}}\right]}\right), \tag{F5}$$

where f_{EC} describes the efficiency of the error correction.

Finally, in this simple model, the targets of the linear programs [Eqs. (25) and (26)] fulfill

$$y_{\alpha,1} = 1-(1-p_{\mathrm{d}})^2(1-\eta) \tag{F6}$$

and

$$e_1^{\mathrm{ideal}} = p_{\mathrm{d}}^2\frac{1}{2} + p_{\mathrm{d}}(1-p_{\mathrm{d}})(1-\eta) + p_{\mathrm{d}}(1-p_{\mathrm{d}})\eta\frac{1}{2}. \tag{F7}$$

While Eq. (F6) follows trivially, Eq. (F7) reflects the fact that, in the model, a perfect single-photon state (i.e., $|\mathrm{H}\rangle$ or $|\mathrm{V}\rangle$) can only trigger an error if either both detectors experience a dark count—which happens with a probability of p_{d}^2—or only the wrong detector experiences a dark count—which happens with a probability of $p_{\mathrm{d}}(1-p_{\mathrm{d}})$. Conditioned on the first event, the error probability is $1/2$, because double clicks are randomly assigned to a specific outcome. Conditioned on the second event, an error occurs if either the photon is lost (corresponding to the $(1-\eta)$ term) or the photon is not lost and thus fires the correct detector but the resulting double click results in a bit error through the random assignment (corresponding to the $\eta/2$ term).

We remark that Eqs. (F6) and (F7) provide the estimates that one would obtain in the perfect PE limit, which is plotted in Fig. 3 of the main text for comparison purposes.

[1] C. Portmann and R. Renner, Security in quantum cryptography, Rev. Mod. Phys. **94**, 025008 (2022).

[2] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing. *In Proceedings IEEE International Conference on Computers, Systems & Signal Processing*, 175–179 (IEEE, NY, Bangalore, India, 1984).

[3] https://www.idquantique.com.

[4] https://www.global.toshiba/ww/products-solutions/security-ict/qkd.html.

[5] https://qubridge.io/.

[6] https://www.thinkquantum.com/.

[7] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, and J. F. Dynes, The SECOQC quantum key distribution network in Vienna, New J. Phys. **11**, 075001 (2009).

[8] F. Xu, *et al.*, Field experiment on a robust hierarchical metropolitan quantum cryptography network, Chin. Sci. Bull. **54**, 2991 (2009).

[9] M. Sasaki *et al.*, Field test of quantum key distribution in the Tokyo QKD Network, Opt. Express **19**, 10387 (2011).

[10] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, and P. Monbaron, Long-term performance of the SwissQuantum quantum key distribution network in a field environment, New J. Phys. **13**, 123001 (2011).

[11] Y.-A. Chen *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature **589**, 214 (2021).

[12] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[13] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, Quantum key distribution with correlated sources, Sci. Adv. **6**, eaaz4487 (2020).

[14] V. Zapatero, Á. Navarrete, K. Tamaki, and M. Curty, Security of quantum key distribution with intensity correlations, Quantum **5**, 602 (2021).

[15] X. Sixto, V. Zapatero, and M. Curty, Security of decoy-state quantum key distribution with correlated intensity fluctuations, Phys. Rev. Appl. **18**, 044069 (2022).

[16] A. Vakhitov, V. Makarov, and D. R. Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, J. Mod. Opt. **48**, 2023 (2001).

[17] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).

[18] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Risk analysis of Trojan-horse attacks on practical quantum key distribution systems, IEEE J. Sel. Top. Quantum Electron. **21**, 168 (2014).

[19] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, New J. Phys. **16**, 123030 (2014).

[20] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, Invisible Trojan-horse attack, Sci. Rep. **7**, 1 (2017).

[21] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Practical security bounds against the Trojan-horse attack in quantum key distribution, Phys. Rev. X **5**, 031030 (2015).

[22] K. Tamaki, M. Curty, and M. Lucamarini, Decoy-state quantum key distribution with a leaky source, New J. Phys. **18**, 065008 (2016).

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

[24] Á. Navarrete and M. Curty, Improved finite-key security analysis of quantum key distribution against Trojan-horse attacks, Quantum Sci. Technol. **7**, 035021 (2022).

[25] M. Curty, T. Moroder, X. Ma, and N. Lütkenhaus, Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution, Opt. Lett. **34**, 3238 (2009).

[26] M. Curty, X. Ma, B. Qi, and T. Moroder, Passive decoy-state quantum key distribution with practical light sources, Phys. Rev. A **81**, 022310 (2010).

[27] Y. Li, W. S. Bao, H. W. Li, C. Zhou, and Y. Wang, Passive decoy-state quantum key distribution using weak coherent pulses with intensity fluctuations, Phys. Rev. A **89**, 032329 (2014).

[28] Y. Z. Shan, S. H. Sun, X. C. Ma, M. S. Jiang, Y. L. Zhou, and L. M. Liang, Measurement-device-independent quantum key distribution with a passive decoy-state method, Phys. Rev. A **90**, 042334 (2014).

[29] Y. Zhang, W. Chen, S. Wang, Z.-Q. Yin, F.-X. Xu, X.-W. Wu, C.-H. Dong, H.-W. Li, G.-C. Guo, and Z.-F. Han, Practical non-Poissonian light source for passive decoy state quantum key distribution, Opt. Lett. **35**, 3393 (2010).

[30] Y. Zhang, S. Wang, Z.-Q. Yin, W. Chen, W.-Y. Liang, H.-W. Li, G.-C. Guo, and Z.-F. Han, Experimental demonstration of passive decoy state quantum key distribution, Chin. Phys. B **21**, 100307 (2012).

[31] S. Krapick, M. S. Stefszky, M. Jachura, B. Brecht, M. Avenhaus, and C. Silberhorn, Bright integrated photon-pair source for practical passive decoy-state quantum key distribution, Phys. Rev. A **89**, 012329 (2014).

[32] Q.-C. Sun, W.-L. Wang, Y. Liu, F. Zhou, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Chen, X. Ma, Q. Zhang, Experimental passive decoy-state quantum key distribution, Laser Phys. Lett. **11**, 085202 (2014).

[33] S. H. Sun, G. Z. Tang, C. Y. Li, and L. M. Liang, Experimental demonstration of passive-decoy-state quantum key distribution with two independent lasers, Phys. Rev. A **94**, 032324 (2016).

[34] M. Curty, X. Ma, H.-K. Lo, and N. Lütkenhaus, Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals, Phys. Rev. A **82**, 052325 (2010).

[35] W. Wang, R. Wang, C. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, and H.-K. Lo, Fully-passive quantum key distribution, Phys. Rev. Lett. **130**, 220801 (2023).

[36] V. Zapatero, W. Wang, and M. Curty, A fully passive transmitter for decoy-state quantum key distribution, Quantum Sci. Technol. **8**, 025014 (2023).

[37] F. Y. Lu *et al.*, Experimental demonstration of fully passive quantum key distribution, Phys. Rev. Lett. **131**, 110802 (2023).

[38] C. Hu, W. Wang, K. S. Chan, Z. Yuan, and H.-K. Lo, Proof-of-principle demonstration of fully-passive quantum key distribution, Phys. Rev. Lett. **131**, 110801 (2023).

[39] W. Wang, R. Wang, and H.-K. Lo, Fully-passive twin-field quantum key distribution, https://arxiv.org/abs/2304.12062 (2023).

[40] A. Huang, S. Barz, E. Andersson, and V. Makarov, Implementation vulnerabilities in general quantum cryptography, New J. Phys. **20**, 103016 (2018).

[41] G. L. Long and X. S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, Phys. Rev. A **65**, 032302 (2002).

[42] J. Wu, G. L. Long, and M. Hayashi, Quantum secure direct communication with private dense coding using a general preshared quantum state, Phys. Rev. Appl. **17**, 064011 (2022).

[43] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[44] G. Kato, Concentration inequality using unconfirmed knowledge, https://arxiv.org/abs/2002.04357 (2020).

[45] T. Metger, O. Fawzi, D. Sutter, and R. Renner, Generalised entropy accumulation. *In 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science*, 844–850 (2022).

[46] T. Metger and R. Renner, Security of quantum key distribution from generalised entropy accumulation, Nat. Commun. **14**, 5272 (2023).

[47] J. L. Carter and M. N. Wegman, Universal classes of hash functions. *In Proceedings of the 9th annual ACM symposium on theory of computing*, 106–112 (1977).

[48] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover hashing against quantum side information, IEEE Trans. Inf. Theory **57**, 5524 (2011).

[49] Namely, for, say, the first interval, we are asserting that $\Pr\left[N q_{\mathrm{key}} \left\langle 1\right\rangle_{\Omega_j^{\mathrm{key}}} Q_j^{\mathrm{key}} \in \left(K^{\mathrm{L}}_{N,\epsilon}(M_j^{\mathrm{key}}), K^{\mathrm{lU}}_{N,\epsilon}(M_j^{\mathrm{key}})\right)\right] \geq 1 - 2\epsilon$.

[50] C. Bonferroni, Teoria statistica delle classi e calcolo delle probabilita, Pubblicazioni del R Istituto Superiore di Scienze Economiche e Commericiali di Firenze **8**, 3 (1936).

[51] Note that Eq. (23) trivially holds if we consider closed intervals instead, which we do for the LPs.

[52] R. J. Serfling, Probability inequalities for the sum in sampling without replacement, Ann. Stat. **2**, 39 (1974).

[53] X. Sixto, G. Currás-Lorenzo, K. Tamaki, and M. Curty, Secret key rate bounds for quantum key distribution with faulty active phase randomization, EPJ Quantum Technol. **10**, 1 (2023).

[54] S. H. Sun, M. Gao, M. S. Jiang, C. Y. Li, and L. M. Liang, Partially random phase attack to the practical two-way quantum-key-distribution system, Phys. Rev. A **85**, 032304 (2012).

[55] S. H. Sun, F. Xu, M. S. Jiang, X. C. Ma, H. K. Lo, and L. M. Liang, Effect of source tampering in the security of quantum cryptography, Phys. Rev. A **92**, 022304 (2015).

[56] A. Huang, Á. Navarrete, S. H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Laser-seeding attack in quantum key distribution, Phys. Rev. Appl. **12**, 064043 (2019).

[57] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge (UK), 2000).

[58] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 1 (2012).

[59] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, Chain rules for smooth min-and max-entropies, IEEE Trans. Inf. Theory **59**, 2603 (2013).

[60] M. Tomamichel and R. Renner, Uncertainty relation for smooth entropies, Phys. Rev. Lett. **106**, 110506 (2011).

[61] M. Tomamichel and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, Quantum **1**, 14 (2017).

[62] J. H. Lint, *Introduction to Coding Theory* (Springer-Verlag, Berlin, Berlin, 1999).

[63] M. Tomamichel, Ph.D. thesis, ETH Zurich, 2012.

[64] M. Tomamichel, *Quantum Information Processing With Finite Resources: Mathematical Foundations*. SpringerBriefs in Mathematical Physics **5**, Springer International Publishing (2016).

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