Editors' Suggestion

Improving key rates of the unbalanced phase-encoded BB84 protocol using the flag-state squashing model

Nicky Kai Hong Li and Norbert Lütkenhaus
Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada

(Received 30 July 2020; accepted 2 October 2020; published 2 November 2020)

All phase-encoded BB84 implementations have signal states with unbalanced amplitudes in practice. Thus the original security analyses *a priori* do not apply to them. Previous security proofs use signal tagging of multiphoton pulses to recover the behavior of regular BB84. This is overly conservative as for unbalanced signals the photon number splitting attack does not leak full information to Eve. In this work we exploit the flag-state squashing model to preserve some parts of the multiphoton-generated private information in our analysis. Using a numerical proof technique we obtain significantly higher key rates compared with previously published results in the low-loss regime. It turns out that the usual scenario of untrusted dark counts runs into conceptual difficulties in some parameter regimes. Thus we discuss the trusted dark-count scenario in this paper as well. We also report a gain in key rates when part of the total loss is known to be induced by a trusted device. We highlight that all these key rate improvements can be achieved without modification of the experimental setup.

DOI: 10.1103/PhysRevResearch.2.043172

I. INTRODUCTION

The earliest phase-encoding quantum key distribution (QKD) scheme was proposed by Bennett [1] in 1992 as a demonstration that any two nonorthogonal states can be used for generating shared secret keys between two parties. Later, Townsend [2] and then Hughes *et al.* [3] proposed a more practical phase-encoding Bennett-Brassard 1984 (BB84) protocol which uses two Mach-Zehnder interferometers. In practice, the phase modulator in each Mach-Zehnder unit will introduce photon loss, thereby causing an asymmetry between the intensities of the phase-encoded pulse and the reference pulse even if the typical observations do not directly reveal this. This asymmetric loss was addressed in Refs. [4–6] which model the loss caused by an imperfect phase modulator with a beam splitter (BS) of the same transmission probability.

The first attempt in giving security proofs for this protocol was made by Ref. [4]. Formal security proofs were later on provided by Refs. [5,6], which both used qubit-based reduction proof techniques. Despite being a deviation from the standard BB84 protocol, Ref. [6] confirms that the old security analysis for the balanced protocol still holds in the unbalanced case. This calls for a revision of the security statement made by Ref. [5], which we will discuss in detail in Sec. VI.

Both Refs. [5] and [6] use decoy states [7–9], signal tagging [10,11], and the qubit squashing model [10,12–14] to convert the full security analysis into an effective qubit-to-qubit security analysis problem. Because of the asymmetric intensities of the signal states, the photon number splitting (PNS) attack [15] will not leak full information of the signal's multiphoton part to Eve since in this case, a single photon obtained in the PNS attack will be in one of two nonorthogonal states, even after basis announcements. Thus, the tagging approach, which pessimistically assumes that all multiphoton signals leak their full information to an adversary, simplifies the security proof but underestimates the secure key rate of this protocol.

In this paper, we will answer the following questions: Could we improve the key rates in Ref. [6] if we keep the multiphoton part of the signals? Could the multiphoton part of the signal contribute significantly to key rates when the total loss or the asymmetry is large?

To highlight the differences between our approach and that of Refs. [5,6], we apply the numerical analysis formulated in Ref. [16], which involves optimizations over finite-dimensional matrices to obtain reliable lower bounds on the key rates. On the source side, we treat lower photon numbers explicitly, while turning to tagging again for higher photon numbers. On the receiver side, we know that the qubit squashing model converts the multiclick events caused by the multiphoton part of the signals into additional qubit errors [5,13,14]. The convenience of reaching a qubit picture may thus cost a reduction in key rate. Therefore, we use the flag-state squashing model [17] to circumvent this problem, especially for low-loss channels. The flag-state squashing model preserves any measurement on a low photon-number subspace, while tagging the arriving signals of higher photon numbers. As a result, we obtain secret key rates that can exceed the ones quoted in Refs. [5,6].

During our investigations, we noticed a problem with the common approach which attributes all observed errors to an

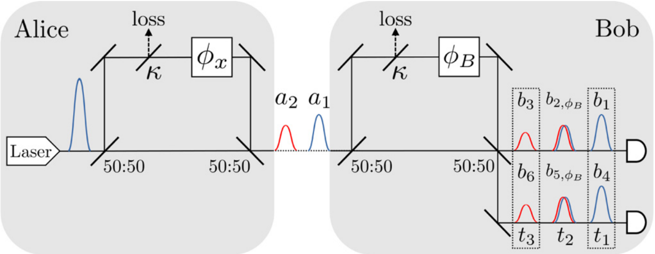


FIG. 1. The setup for the unbalanced phase-encoded BB84 protocol. All beam splitters (BSs) are labeled by their transmissivities. The grouping of Bob's detection events are represented by the dotted boxes.

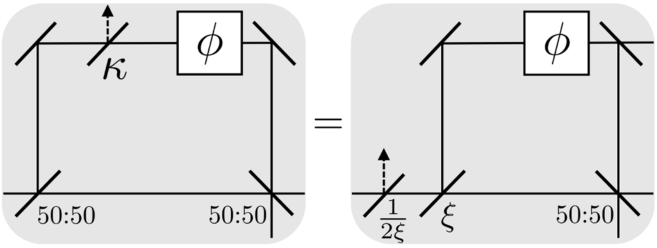


FIG. 2. Equivalence relationship between a lossy phase modulator in the encoding device and an uneven BS with transmissivity $\frac{1}{2\xi}$ followed by another uneven BS with transmissivity ξ and a perfect phase modulator, where $\xi = \frac{1}{1+\kappa}$ [5].

adversary and describes Bob's detection device by an idealized setup. Once the actual detectors have some dark-count rate, this approach may lead in some circumstances to unphysical constraints, meaning that such an ideal device could not lead to the actual observations. For that reason, we will also introduce results for trusted detector noises, especially dark counts, for which this problem does not exist.

The rest of this paper is outlined as follows. We first revisit the protocol in Sec. II and describe the mathematical model of the protocol in Sec. III. We will then justify our security proof techniques and state the methods that allow us to speed up our key rate computations in Sec. IV. With the description of how we simulate experimental statistics in Sec. V, we present our lower bounds for the secure key rates of the protocol in Sec. VI. A summary of our results is provided in Sec. VII to conclude this paper. Full justifications of the proof techniques mentioned in Sec. IV are discussed in the Appendixes.

II. PROTOCOL DESCRIPTION

We consider a phase-encoded BB84 protocol with a Mach-Zehnder setup. The only modification is that we take into account the typical loss in one arm of the interferometer, which results from the insertion loss of phase modulators. This asymmetric loss leads to an unbalance of the amplitudes of the two generated pulses as illustrated in Fig. 1. We describe here the general outline of the protocol structure. Since we are dealing with the asymptotic key rate in this article, we omit any detail that would be relevant only for a finite-size analysis of the protocol.

(1) *State preparation*: Alice prepares a phase-randomized coherent state with mean photon number $|\alpha|^2$ where $\alpha \in \mathbb{C}$ and chooses a random phase ϕ_x from the set $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ with equal probabilities in each round. Alice also sends a small portion of decoy coherent states with different mean photon numbers $\{|\alpha_i|^2 : \forall \alpha_i \in \mathbb{C}\}_{i\in\mathbb{N}}$.

(2) *Measurement*: Once Bob receives the signal state, he chooses a random phase ϕ_B from the set $\{0, \frac{\pi}{2}\}$ with equal probabilities and records all events coming from the two detectors at any of the three time slots. A click is termed "outside" if it is not in the second (middle) time slot.

(3) *Testing*: After repeating steps 1 and 2 for many times, Alice and Bob jointly announce a random subset of their data (including events coming from decoy states) and decide whether they should abort or proceed with the rest of the protocol.

(4) *Announcement, sifting, and postselection*: For each round, Alice announces the basis to be "even" if she picks her phase from $\{0, \pi\}$ or she announces "odd" if her phase is in $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$. Bob announces "even" if he picks $\phi_B = 0$ or "odd" if $\phi_B = \frac{\pi}{2}$. In addition to basis announcements, Bob also announces "discard" for events that have only outside clicks or no click. Alice keeps the ϕ_x only for the rounds where Bob did not announce "discard" and where her bases match with Bob's. Bob keeps a detection event if his basis matches Alice's and the event is not to be discarded.

(5) *Direct reconciliation key map*: Alice maps $\phi_x^{(j)}$ in the jth kept rounds to the jth bit z_j of the raw key as

$$z_j = \begin{cases} 0, & \text{if } \phi_x^{(j)} = 0, \pi/2, \\ 1, & \text{if } \phi_x^{(j)} = \pi, 3\pi/2. \end{cases} \tag{1}$$

(6) *Error correction and privacy amplification*: Alice and Bob perform standard error correction so that Bob also obtains a copy of the key map register. They then proceed with a privacy amplification protocol to obtain a shared secret key.

We point out that our method generalizes to any asymmetric basis choice (i.e., probabilities of choosing "even" and "odd" bases are not equal). It was shown in Ref. [18] that the probability of choosing one basis can be set arbitrarily close to 1 without affecting the asymptotic security analysis. Note that the formalism described here would also allow one to consider the reverse reconciliation approach, where in step 5 of the protocol Bob performs a key map instead of Alice. Then, Alice and Bob would have to swap their respective roles in step 6.

III. MATHEMATICAL MODEL OF THE PROTOCOL

A. Optical models

We start by identifying two equivalent optical models for the Mach-Zehnder component that appears in both Alice's and Bob's apparatus. The descriptions for the two models are illustrated in Fig. 2. Instead of having the loss in one arm of the interferometer, the equivalent model places a loss element in front of the Mach-Zehnder component, which then has an asymmetric beam splitter at the entry [5].

This replacement picture tells us that Alice's loss can be absorbed into the rescaled amplitude of the incoming single laser pulse, whereas Bob's loss can be absorbed into the channel's action.

B. State preparation

We use the source-replacement scheme [19,20] to represent a prepare-and-measure scheme with an entanglement-based scheme. Since Alice's signal state is mixed, we will introduce a purifying "shield" system that will be left behind in the source so that the existing source-replacement framework can be applied. We will provide a detailed description of the entangled pure state prepared by Alice below.

To prepare the output signal state, Alice's laser first creates a phase-randomized coherent state

$$\sigma_{\text{in}}(2\alpha) = \int_0^{2\pi} \frac{d\theta}{2\pi} |2\alpha e^{i\theta}\rangle\langle 2\alpha e^{i\theta}| = \sum_{n=0}^{\infty} p_n(2\alpha)|n\rangle\langle n|, \quad (2)$$

where $p_n(\beta) = e^{-|\beta|^2}\frac{|\beta|^{2n}}{n!}$ is the Poissonian distribution in photon number n. She then sends it through her encoding device set at a phase ϕ_x which outputs a time-bin signal with two modes,

$$\sigma_x(\alpha) = \int_0^{2\pi} \frac{d\theta}{2\pi} \left|\psi_x^\theta(\alpha)\right\rangle\!\left\langle\psi_x^\theta(\alpha)\right|, \quad (3)$$

where $|\psi_x^\theta(\alpha)\rangle = |\alpha e^{i\theta}, \sqrt{\kappa}\,\alpha e^{i(\theta-\phi_x)}\rangle$.

In the following steps, we will express the state $\sigma_x(\alpha)$ in a two-mode Fock basis $\{|s_n^x(\xi)\rangle\}$ which is defined later in Eq. (8). Let $\widetilde{a}_1^\dagger$ and $\widetilde{a}_2^\dagger$ be the creation operators of the two output time modes of the signal. We define a rescaled amplitude $\widetilde{\alpha} := \alpha\sqrt{1+\kappa} = \alpha/\sqrt{\xi}$ with the definition $\xi := \frac{1}{1+\kappa}$ and a new mode creation operator

$$\widetilde{a}_{\theta,x}^\dagger := \frac{1}{\widetilde{\alpha}}(\alpha e^{i\theta}\,\widetilde{a}_1^\dagger + \sqrt{\kappa}\,\alpha e^{i(\theta-\phi_x)}\,\widetilde{a}_2^\dagger) \quad (4)$$

$$= \frac{e^{i\theta}}{\sqrt{1+\kappa}}(\widetilde{a}_1^\dagger + \sqrt{\kappa}\,e^{-i\phi_x}\,\widetilde{a}_2^\dagger) \quad (5)$$

$$= e^{i\theta}(\sqrt{\xi}\,\widetilde{a}_1^\dagger + \sqrt{1-\xi}\,e^{-i\phi_x}\,\widetilde{a}_2^\dagger). \quad (6)$$

We define a set of two-mode Fock states for $n \in \mathbb{N}$ as

$$|s_n^x(\xi)\rangle = \frac{1}{\sqrt{n!}}(\widetilde{a}_{\theta=0,x}^\dagger)^n|0\rangle \quad (7)$$

$$= \sum_{k=0}^{n}\sqrt{\binom{n}{k}}\,\xi^{\frac{n-k}{2}}(1-\xi)^{\frac{k}{2}}e^{-ik\phi_x}|n-k,k\rangle, \quad (8)$$

The state $|\psi_x^\theta(\alpha)\rangle$ can be rewritten in the new basis as

$$|\psi_x^\theta(\alpha)\rangle = e^{-\frac{|\widetilde{\alpha}|^2}{2}}\sum_{n=0}^{\infty}\frac{\widetilde{\alpha}^n}{n!}(\widetilde{a}_{\theta,x}^\dagger)^n|0\rangle = e^{-\frac{|\widetilde{\alpha}|^2}{2}}\sum_{n=0}^{\infty}\frac{(\widetilde{\alpha}e^{i\theta})^n}{\sqrt{n!}}|s_n^x(\xi)\rangle \quad (9)$$

which is a coherent state with amplitude $\widetilde{\alpha}$. The phase-randomized signal state is therefore a Poissonian mixture of the new Fock states as in

$$\sigma_x(\alpha) = \sum_{n=0}^{\infty} p_n(\widetilde{\alpha})|s_n^x(\xi)\rangle\langle s_n^x(\xi)|. \quad (10)$$

Since the signal state $\sigma_x(\alpha)$ is mixed, Alice can purify the state by introducing an ancillary system A_S such that the following is a pure state,

$$|\sigma_x(\alpha)\rangle_{A_SA'} = \sum_{n=0}^{\infty}\sqrt{p_n(\widetilde{\alpha})}\;|n\rangle_{A_S}\otimes\left|s_n^x(\xi)\right\rangle_{A'}\;, \quad (11)$$

where the register A' is the signal system. Note that the probability $p_n(\widetilde{\alpha})$ is independent of Alice's choice x.

We can thus summarize the source description as Alice preparing an entangled pure state

$$|\Psi\rangle_{AA_SA'} = \sum_x \sqrt{p_x}\;|x\rangle_A\otimes|\sigma_x(\alpha)\rangle_{A_SA'}\;, \quad (12)$$

where $\{|x\rangle_A\}_{x=0,\dots,3}$ is an orthonormal basis of Alice's register A for x corresponding to the phase $\phi_x = \frac{\pi}{2}x$ and $p_x = \frac{1}{4}$ for all $x \in \{0, 1, 2, 3\}$. Note that registers A and A_S are private to Alice, and Eve only has access to the signal system A'. We call the purifying system A_S a "shield" system for it to be inaccessible to Eve [i.e., Eve only gets the mixed state $\sigma_x(\alpha)$ but not the pure state $|\sigma_x(\alpha)\rangle_{A_SA'}$].

C. Measurements

In the prepare-and-measure scheme, the action of Alice randomly choosing the phase ϕ_x in the signal state is equivalent to a measurement on $|\Psi\rangle_{AA_SA'}$ with positive operator-valued measure (POVM) $\{|x\rangle\langle x|_A\}_{x=0,\dots,3}$. Alice's measurement can be performed before or after Bob performs his measurement.

We start out by describing the POVM of Bob's measurement assuming ideal devices, especially without dark counts of the detectors. We will later on derive the POVM of devices with specified dark counts. To characterize all of Bob's possible measurement outcomes, we construct his POVM using the creation and annihilation operators for six optical modes arriving at three different time slots and at two detectors. Ignoring global phases, the six annihilation operators of a fixed phase ϕ_B, which correspond to the six "click" locations depicted in Fig. 1, are

$$b_1 = b_4 \to \sqrt{\frac{\xi}{2}}\;a_1\;, \quad (13)$$

$$b_3 = b_6 \to \sqrt{\frac{1-\xi}{2}}\;a_2\;, \quad (14)$$

$$b_{2,\phi_B} \to \sqrt{\frac{1-\xi}{2}}\;a_1 - e^{i\phi_B}\sqrt{\frac{\xi}{2}}\;a_2\;, \quad (15)$$

$$b_{5,\phi_B} \to \sqrt{\frac{1-\xi}{2}}\;a_1 + e^{i\phi_B}\sqrt{\frac{\xi}{2}}\;a_2\;, \quad (16)$$

where a_1 and a_2 are annihilation operators of the two incoming time modes of the signal.

Since $b_1 = b_4$ and $b_3 = b_6$, the POVM elements corresponding to click events at 1 and 4 (3 and 6) are the same. Hence, each pair can be combined into a single time-mode annihilation operator. The corresponding operators for the two pairs are

$$b_{t_1} \to \sqrt{\xi}\;a_1\;,\quad b_{t_3} \to \sqrt{1-\xi}\;a_2, \quad (17)$$

where t_1 and t_3 denote the first and third time slots in Fig 1. This is equivalent to coarse graining the outside-only click

POVM elements and outcome probabilities but without losing information about the relative phase, $\phi_x - \phi_B$. This reduces the redundancy in constraints for the optimization, which will be described in Sec. IV C.

As Bob's measurement outcomes consist of all combinations of click events at different time slots, detectors, and basis choices, his POVM elements are obtained by summing weighted projectors of all possible states that could lead to a particular click pattern. Based on the fact that Bob uses threshold detectors for detection, all POVM elements are block diagonal in total photon number basis [12,13].

These allow the construction of Bob's POVM elements in terms of the modes impinging on the detectors by first restricting to the n-total photon subspace of Bob's entire system and defining the following operators corresponding to different click events:

(1) no click (for $n = 0$):

$$F_0^{\phi_B} = p(\phi_B)|0\rangle\langle 0|, \tag{18}$$

(2) single click (for $n \geqslant 1$):

$$F_{i_1}^{n,\phi_B} = p(\phi_B)\frac{1}{n!}(b_{i_1}^{\dagger})^n|0\rangle\langle 0|b_{i_1}^n \ , \tag{19}$$

(3) double click (for $n \geqslant 2$):

$$F_{i_1,i_2}^{n,\phi_B} = p(\phi_B)\sum_{k=1}^{n-1}\frac{(b_{i_1}^{\dagger})^{n-k}(b_{i_2}^{\dagger})^k|0\rangle\langle 0|b_{i_1}^{n-k}\ b_{i_2}^k}{(n-k)!\ k!}\ , \tag{20}$$

(4) triple click (for $n \geqslant 3$):

$$F_{i_1,i_2,i_3}^{n,\phi_B} = p(\phi_B)\sum_{k=1}^{n-2}\ \sum_{j=1}^{n-k-1}\ |\beta_3(n,j,k)\rangle\langle\beta_3(n,j,k)| \tag{21}$$

with $|\beta_3(n,j,k)\rangle = \frac{(b_{i_1}^{\dagger})^{n-k-j}(b_{i_2}^{\dagger})^k(b_{i_3}^{\dagger})^j|0\rangle}{\sqrt{(n-k-j)!\ k!\ j!}}$,

(5) all click (for $n \geqslant 4$):

$$F_{\text{ac}}^{n,\phi_B} = p(\phi_B)\sum_{k=1}^{n-3}\ \sum_{j=1}^{n-k-2}\ \sum_{l=1}^{n-k-j-1}\ |\beta_4(n,j,k,l)\rangle \times\langle\beta_4(n,j,k,l)| \tag{22}$$

with $|\beta_4(n,j,k,l)\rangle = \frac{(b_{i_1}^{\dagger})^{n-k-j-l}(b_{i_2}^{\dagger})^k(b_{i_3}^{\dagger})^j(b_{i_4}^{\dagger})^l|0\rangle}{\sqrt{(n-k-j-l)!\ k!\ j!\ l!}}$, where $p(\phi_B)$ is the probability of choosing the phase ϕ_B and $b_{i_\mu}^{\dagger} \in \{b_{t_1}^{\dagger}, b_{2,\phi_B}^{\dagger}, b_{5,\phi_B}^{\dagger}, b_{t_3}^{\dagger}\}$ are the mode creation operators for a fixed phase ϕ_B, with $b_{i_\mu}^{\dagger} \neq b_{i_\nu}^{\dagger}$ for all $\mu \neq \nu$ and $\mu, \nu \in \{1, 2, 3, 4\}$. We can express Bob's POVM elements in terms of the incoming modes, a_1 and a_2, by substituting the final modes with Eqs. (15)–(17).

To obtain Bob's POVM elements for the full Hilbert space, one simply sums over all contributions from all photon number subspaces to get

$$F_k = \sum_{n=0}^{\infty} F_k^n\ , \tag{23}$$

where k labels the 16 possible click patterns (Bob's measurement outcomes) in each of the two measurement bases. For n to be less than the minimum photon number to trigger the click event k, F_k^n is a zero operator. If k is the no-click event, F_k^n is a zero operator for all $n \geqslant 1$.

To reduce the number of linearly dependent POVM elements for better numerical performance in calculating key rates [21], we combine the pairs of ϕ_B-independent POVM elements of the two measurement bases into one by summing the two elements together. This reduces the cardinality of Bob's POVM from 32 to 28 since four click patterns (no click, t_1 only, t_3 only, and $t_1 + t_3$) are basis independent.

In a trusted dark-count scenario where dark counts are not controlled by Eve, we incorporate the effect of dark counts into Bob's POVM by applying a classical postprocessing map, $\mathcal{P}$, on Bob's POVM elements $\{F_k\}$. The output of the map is a new POVM $\{P_k\}$ with each element corresponding to a linear combination of the original POVM such that $P_k = \sum_i \mathcal{P}_{k,i}\ F_i$, where $\mathcal{P}_{k,i}$ are the matrix elements of the linear map $\mathcal{P}$. We illustrate the action of the map $\mathcal{P}$ with the new POVM elements in Eqs. (A3)–(A9). Since the map $\mathcal{P}$ acts the same on all photon-number subspaces, it also holds that

$$P_k^n = \sum_i \mathcal{P}_{k,i}\ F_i^n\ . \tag{24}$$

The map $\mathcal{P}$ models the effect of dark counts as a classical noise in the sense that for each detector and at each detection time window, a no-click event flips to a click event with probability p_d. We can recover Bob's dark-count-free POVM $\{F_k\}$ by setting the dark-count probability $p_d = 0$ in the case with untrusted dark counts.

Overall, we obtain the joint POVM of Alice's and Bob's measurements $\{|x\rangle\langle x|_A \otimes P_k\}$ where $x \in \{0, ..., 3\}$ and $k \in \{1, ..., 28\}$ since Bob has 28 coarse-grained outcomes in total if no-click cases are included.

IV. SECURITY PROOF TECHNIQUES

A. Flag-state squashing model

In order to numerically compute the secure key rate, we need to reduce the dimension of Bob's state from infinite to finite so that numerical optimization solvers can be used. Since Bob uses threshold detectors, his POVM elements are block diagonal, so the qubit squashing model [5,12–14] can be applied. However, by reassigning the multiclick events to single-click events randomly, the squashing model introduces additional qubit errors to the original data. Instead, the flag-state squashing model [17] is used here to circumvent this problem.

We set a finite photon-number cutoff N_B and define the $(n \leqslant N_B)$-photon and $(n > N_B)$-photon subspaces to be two Hilbert spaces containing Fock states of at most N_B and at least $N_B + 1$ photons respectively. The flag-state squashing map Λ first projects Bob's state ρ onto the two subspaces. It then applies an identity map to the projected state $\rho_{n\leqslant N_B}$ and measures the projected state $\rho_{n>N_B}$ with the POVM $\{P_k\}$ to give the squashed state

$$\Lambda(\rho) = \begin{pmatrix}\rho_{n\leqslant N_B} & 0\\ 0 & \sum_k \mathrm{Tr}(P_k\ \rho_{n>N_B})|k\rangle\langle k|\end{pmatrix}. \tag{25}$$

Bob's corresponding flag-state squashed POVM elements are

$$\widetilde{P}_k = \left(\sum_{n=0}^{N_B} P_k^n\right) \oplus |k\rangle\langle k|, \tag{26}$$

where N_B is a finite-number photon cutoff and k labels Bob's detection events. The joint POVM of Alice's and Bob's measurements in the flag-state squashing model is $\{|x\rangle\langle x|_A \otimes \widetilde{P}_k\}$, where $x \in \{0, ..., 3\}$ and $k \in \{1, ..., 28\}$.

Since the measurement channel acting on the $(n > N_B)$-photon subspace is entanglement breaking [22], one needs to find the lower bound for $\mathrm{Tr}(\Pi_{n \leqslant N_B}\, \rho)$ with Bob's measurement statistics to ensure that some entanglement between Alice and Bob is preserved in order for them to establish a secret key [20]. For trusted dark counts, we show in Appendix A that the lower bound for the weight of the $(n \leqslant N_B)$-photon signal subspace conditioned on Alice choosing signal x is given by

$$p(n \leqslant N_B|x) \geqslant 1 - \frac{p(\mathrm{cc}|x) - p(\mathrm{cc}|0)}{p_{\min}(\mathrm{cc}|N_B+1) - p(\mathrm{cc}|0)}\ , \qquad (27)$$

$$p(\mathrm{cc}|0) = 1 - (1-p_d)^2[1 + p_d(1-p_d)^2(2-p_d)], \qquad (28)$$

$$p_{\min}(\mathrm{cc}|n) = 1 - (1-p_d)^2\xi^n - (1-p_d)^4(1-\xi)^n, \qquad (29)$$

where the conditional cross-click probability, $p(\mathrm{cc}|x)$, is the sum of the observed probabilities of all events excluding no-click events, events with clicks only in time slot t_2 (inside only), and events with clicks only in time slots t_1, t_3 (outside only) given that Alice picks signal x. We also show in Appendix A that the bound in (27) is always tighter than the dark-count-free bound ($p_d = 0$) derived by Narashimhachar [14], so we could also obtain a lower bound of the secure key rate using that dark-count-free bound. For untrusted dark counts, one simply has to use that bound.

B. Decoy state and decomposition of key rate formula

In this article, we prove the security of the protocol against any collective attack. Since the signal states and measurements are permutation invariant between different rounds, the quantum de Finetti theorem [23] or the postselection technique [24] can be applied to uplift our security statement to the security against coherent attacks, which will both lead to the same asymptotic key rate. From that, we obtain a composable ϵ-security proof [25] of the protocol under Eve's general attacks with the same asymptotic key rate as under the collective attack.

Let R be the key register held by Alice in direct reconciliation, E be Eve's quantum and classical register, B be Bob's quantum register, and $\overline{B}$ and $\widetilde{B}$ be Bob's classical registers for his measurement outcomes and announcements respectively. The Devetak-Winter formula [26] for asymptotic secure key rate can be expressed as

$$R_\infty = p_{\mathrm{pass}}[\min_{\rho \in \mathbf{S}} H(R|E) - H(R|\overline{B})], \qquad (30)$$

where p_{pass} is the probability of passing the sifting and postselection steps and $\mathbf{S}$ is the set of all density matrices that satisfy Alice's and Bob's joint statistics.

The key rate formula (30) can be converted into an alternative form, as shown in Refs. [16,27], using the relative entropy

$$R_\infty = \min_{\rho_{AA_SB} \in \mathbf{S}} D(\mathcal{G}(\rho_{AA_SB}) || \mathcal{Z}(\mathcal{G}(\rho_{AA_SB}))) - p_{\mathrm{pass}}\ \delta_{\mathrm{EC}}\ , \qquad (31)$$

where $\mathcal{G}$ and $\mathcal{Z}$ are two maps that will be discussed below. The formula includes a privacy-amplification (PA) term as the first term and an error-correction term $\delta_{\mathrm{EC}} = f_{\mathrm{EC}}\ H(R|\overline{B})$ with a heuristic classical error-correction efficiency factor $f_{\mathrm{EC}} \geqslant 1$.

The $\mathcal{G}$ map is a completely positive trace nonincreasing map capturing the effects of measurements, sifting, postselection, and announcement on Alice's and Bob's joint state, which takes the form [16,28]

$$\mathcal{G}(\rho) = \sum_i K_i\ \rho\ K_i^\dagger \qquad (32)$$

with the Kraus operators of this protocol defined as

$$K_0 = (|0\rangle_R \otimes |0\rangle\langle 0|_A + |1\rangle_R \otimes |2\rangle\langle 2|_A) \otimes \mathcal{F}_0^B \otimes |0\rangle_{\widetilde{B}}, \quad (33)$$

$$K_1 = (|0\rangle_R \otimes |1\rangle\langle 1|_A + |1\rangle_R \otimes |3\rangle\langle 3|_A) \otimes \mathcal{F}_1^B \otimes |1\rangle_{\widetilde{B}}, \quad (34)$$

where $\{|0\rangle_{\widetilde{B}}, |1\rangle_{\widetilde{B}}\}$ is Bob's basis announcement bit, $\mathcal{F}_j^B = \sqrt{\sum_{b \in \mathbf{K}} F_{b,\phi_B = \frac{\pi}{2} j}}$, and $\mathbf{K}$ denotes Bob's postselected outcomes. The $\mathcal{Z}$ map captures the effect of the key map and is given by

$$\mathcal{Z}(\sigma_{RC}) = \sum_{j=0}^{1} (|j\rangle\langle j|_R \otimes \mathbb{1}_C)\ \sigma_{RC}\ (|j\rangle\langle j|_R \otimes \mathbb{1}_C) \qquad (35)$$

with register C encapsulates all registers except R.

Since Alice is sending a Poissonian mixture of Fock states, Eve can, in principle, perform a quantum nondemolition (QND) measurement on Alice's signal to learn its photon number without disturbing the signal itself. We show in Appendix B that as a direct consequence of this the state ρ_{AA_SB} is block diagonal in Alice's output photon number $\widetilde{n}$. Therefore, without loss of generality, we can restrict the minimization in Eq. (31) to be taken over a smaller set $\mathbf{S}' = \{\rho_{AA_SB} \in \mathbf{S} : \rho_{AA_SB} = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\ |\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \rho_{AB}^{\widetilde{n}}\}$ where $\{\rho_{AB}^{\widetilde{n}}\}$ are the normalized states conditioned on Alice sending out $\widetilde{n}$ photons. This allows one to split the PA term into a probabilistic combination of PA terms associated with different $\widetilde{n}$ as in

$$R_\infty = \min_{\rho_{AA_SB} \in \mathbf{S}'} \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\ D\big(\mathcal{G}\big(\rho_{AB}^{\widetilde{n}}\big) \big|\big| \mathcal{Z}\big(\mathcal{G}\big(\rho_{AB}^{\widetilde{n}}\big)\big)\big) - p_{\mathrm{pass}}\ \delta_{\mathrm{EC}}\ . \qquad (36)$$

See Appendix B for the proof of the decomposition.

For our analysis, we assume a decoy-state scenario [7–9], which means that in addition to the usual signal states, Alice prepares also decoy states that are represented by dephased laser pulses with different intensity levels $|\alpha_i|^2$. More precisely, we assume for simplicity the infinite-decoy scenario, where a countably infinite number of decoy intensities are used so that a decoy data analysis can reveal to Alice and Bob the conditional probabilities of any observable, where the condition is with respect to Alice's output photon number $\widetilde{n}$.

These conditional probabilities constrain the feasible set of normalized states $\mathbf{S}_{\widetilde{n}}$ for each of Alice's output photon number $\widetilde{n}$ independently, which further restricts the minimization in Eq. (36) to be taken over a smaller set $\mathbf{S}'' = \{\rho_{AA_SB} \in \mathbf{S} : \rho_{AA_SB} = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\ |\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \rho_{AB}^{\widetilde{n}},\ \ \rho_{AB}^{\widetilde{n}} \in \mathbf{S}_{\widetilde{n}}\ \ \forall\ \ \widetilde{n} \in \mathbb{N}\} \subset \mathbf{S}'$. Given that the probability distribution $\{p_{\widetilde{n}}\}_{\widetilde{n} \in \mathbb{N}}$ is fixed by the intensity of the signal, the minimization over $\mathbf{S}''$ can be pulled into the summation and split into minimizations over individual $\mathbf{S}_{\tilde{n}}$, resulting in the following key rate formula:

$$R_\infty = \sum_{\tilde{n}=0}^{\infty} p_{\tilde{n}} \min_{\rho_{AB}^{\tilde{n}} \in \mathbf{S}_{\tilde{n}}} D\big(\mathcal{G}\big(\rho_{AB}^{\tilde{n}}\big)\big|\big|\mathcal{Z}\big(\mathcal{G}\big(\rho_{AB}^{\tilde{n}}\big)\big)\big) - p_{\text{pass}}\,\delta_{\text{EC}}. \tag{37}$$

We remark that the inclusion of a finite number of decoy states would be a natural extension of this work, in which case the description of each set $\mathbf{S}_{\tilde{n}}$ would depend on other sets $\{\mathbf{S}_{n'} : n' \neq \tilde{n}\}$. Hence, a more careful treatment of the PA term would be needed.

The major benefit of breaking down the PA term into individual minimizations is to avoid the need of keeping the infinite-dimensional shield system A_S in the argument of the optimisation as seen in Eq. (31). Instead of optimizing over the set of infinite-dimensional states, we convert our problem into an infinite number of optimizations with finite-dimensional arguments.

Notice that when Alice sends out vacuum (0 photons), Eve learns nothing about Alice's choice x, so each key bit $z \in \{0, 1\}$ is equally likely to Eve, which implies that $H(R|E) = H(R) = 1$ (see Ref. [29]). Therefore, the first term in the summation in Eq. (37) is equal to $p_{\text{pass}}^{\tilde{n}=0}$ which is the contribution from Alice sending out vacuum to the probability of passing sifting and postselection.

By Klein's inequality, quantum relative entropy is non-negative, i.e., $D(A||B) \geqslant 0$, for all positive semidefinite matrices $A, B \geqslant 0$ such that $\text{Tr}(A) \geqslant \text{Tr}(B)$ [30], so $D(\mathcal{G}(\rho_{AB}^{\tilde{n}})||\mathcal{Z}(\mathcal{G}(\rho_{AB}^{\tilde{n}}))) \geqslant 0 \;\; \forall \;\; \tilde{n} \in \mathbb{N}$. Thus, omitting any terms in the summation will only reduce the total value on the right-hand side of Eq. (37). In fact, omitting an $\tilde{n}$-photon term is the same as treating all $\tilde{n}$-photon output signals as being tagged for which the encoded state is fully known to Eve. Since we can only optimize a finite number of terms in the infinite sum, we can truncate the infinite sum at $\tilde{n} = N_A$ where N_A is a positive finite integer to obtain a lower bound for the key rate. The choice of $N_A = 1$ corresponds to the tagging as used in Refs. [5,6]. We then have the key rate expression as

$$\begin{aligned} R_\infty \geqslant p_{\text{pass}}^{\tilde{n}=0} + \sum_{\tilde{n}=1}^{N_A} p_{\tilde{n}} \min_{\rho_{AB}^{\tilde{n}} \in \mathbf{S}_{\tilde{n}}} D\big(\mathcal{G}\big(\rho_{AB}^{\tilde{n}}\big)\big|\big|\mathcal{Z}\big(\mathcal{G}\big(\rho_{AB}^{\tilde{n}}\big)\big)\big) \\ - p_{\text{pass}}\,\delta_{\text{EC}}\;. \end{aligned} \tag{38}$$

This allows us to reduce the number of finite-dimensional optimizations from infinity to a finite number that corresponds to the limited computational resources available to us.

C. The optimization problem

The convex optimization problem corresponding to each PA term in Eq. (38) can be formulated as

$$\begin{aligned}
&\text{minimize } D(\mathcal{G}(\rho_{AB}^{\tilde{n}})||\mathcal{Z}(\mathcal{G}(\rho_{AB}^{\tilde{n}})))\\
&\text{subject to}\\
&\quad \text{Tr}[(|x\rangle\langle x|_A \otimes \widetilde{P}_k)\;\rho_{AB}^{\tilde{n}}] = p(x, k|\tilde{n}),\\
&\quad \text{Tr}[(|x\rangle\langle x|_A \otimes \Pi_{n\leqslant N_B})\;\rho_{AB}^{\tilde{n}}] \geqslant p(x)\;p_{n\leqslant N_B|x,\tilde{n}}^{\min},\\
&\quad \text{Tr}_B(\rho_{AB}^{\tilde{n}}) = \frac{1}{p_{\tilde{n}}}\text{Tr}_{A_S A'}[(|\tilde{n}\rangle\langle\tilde{n}|_{A_S} \otimes \mathbb{1}_{A'})\;|\Psi\rangle\langle\Psi|_{AA_SA'}],\\
&\quad \text{Tr}(\rho_{AB}^{\tilde{n}}) = 1,\\
&\quad \rho_{AB}^{\tilde{n}} \geqslant 0.
\end{aligned} \tag{39}$$

The first line in the constraints demands the shared state $\rho_{AB}^{\tilde{n}}$ conditioned on Alice sending out $\tilde{n}$ photons to satisfy Alice's and Bob's joint measurement outcome probabilities conditioned on $\tilde{n}$, which are obtained from the infinite-decoy analysis. The second line lower bounds the weight of $\rho_{AB}^{\tilde{n}}$ in the $(n \leqslant N_B)$-photon subspace by Eq. (27) but with the observed cross-click probability conditioned on x also conditioned on $\tilde{n}$ here [i.e., replace $p(\text{cc}|x)$ with $p(\text{cc}|x, \tilde{n})$ in Eq. (27)]. The third line demands that Alice's reduced density matrix is unchanged. The last two lines ensure that $\rho_{AB}^{\tilde{n}}$ is a valid, normalized density matrix.

D. Implementation of numerical security analysis

Following the procedure in Ref. [16], the suboptimal solutions to the convex optimization problem (39) for $1 \leqslant \tilde{n} \leqslant N_A$ are obtained numerically using the MATLAB optimization package CVX and the Frank-Wolfe algorithm [31]. These suboptimal solutions infer the upper bound for the individual privacy amplification terms in Eq. (38). A linearization of each of the optimization problems at its suboptimal solution results in a primal semidefinite programming (SDP) problem which can be further converted into a dual SDP problem. Using the CVX numerical solver again, the dual suboptimal solutions for $1 \leqslant \tilde{n} \leqslant N_A$ provide a reliable lower bound on the whole privacy amplification term.

Solving the convex optimization problem is computationally demanding in terms of time and memory even if the flag-state squashing model is applied to reduce the dimension of the matrix variables $\rho_{AB}^{\tilde{n}}$. One can further utilize the structure of the flag-state squashed state as described in Eq. (25) to reduce the number of complex variables in the allowed matrices $\rho_{AB}^{\tilde{n}}$. Bob's flag-state squashed POVM elements also enable us to split multiplications between constraint matrices and the state variable $\rho_{AB}^{\tilde{n}}$. In addition, the objective function in (39) can be evaluated much faster if the computation is restricted only to the nonzero subspaces in the images of the maps $\mathcal{G}$ and $\mathcal{Z}$. With these three techniques, we managed to reduce the computation time of the convex optimization by a significant amount. See Appendix C for the technical details.

We utilize the fact that the optimization problem specified in (39) is independent of the mean photon number $|\alpha|^2$ of Alice's phase-randomized coherent state because the minimizations in Eq. (37) are over each set $\mathbf{S}_{\tilde{n}}$ separately. In other words, the choice of $|\alpha|^2$ only affects the photon number distribution $\{p_{\tilde{n}}\}$ and the error-correction term δ_{EC} in the key rate formula (38). Therefore, we can maximize the key rate lower bound over the signal intensity $|\alpha|^2$ efficiently once we have the dual suboptimal solutions since the error-correction term can be directly calculated from the observables of the corresponding simulation.

V. SIMULATION OF EXPERIMENTS

In the absence of experimental data, we have to perform a simulation of an experiment to obtain realistic probability distributions which replace the experimental data as input of our security analysis. Note that the details of the simulation model are independent of the actual security proof.

A. Channel simulations and detection efficiency

We simulate the quantum channel between Alice and Bob with a loss-only channel which is essentially an uneven beam splitter. We also assume that both detectors of Bob have equal detection efficiency η_{det}, where each detector can be modeled as a beam splitter with a transmission rate η_{det} followed by an ideal detector. In this simple model, a single parameter η which we call the total transmissivity describes the combined loss caused by the following three effects: the inefficiency in the process of coupling the signal light to the optical fiber, the absorption and scattering processes of light in transmission through the fibre, and the detection efficiency of Bob's threshold detectors.

We also investigate the case where we assume the detection efficiency η_{det} to be outside of Eve's control, as a trusted, characterized loss element of the receiver. In that case, we keep the beam splitter with transmissivity η_{det} in Bob's apparatus, which in turn modifies the POVM elements described in Sec. III C. Bob's POVM with known detection efficiency can be obtained with a similar approach used in Ref. [17].

B. Dark counts

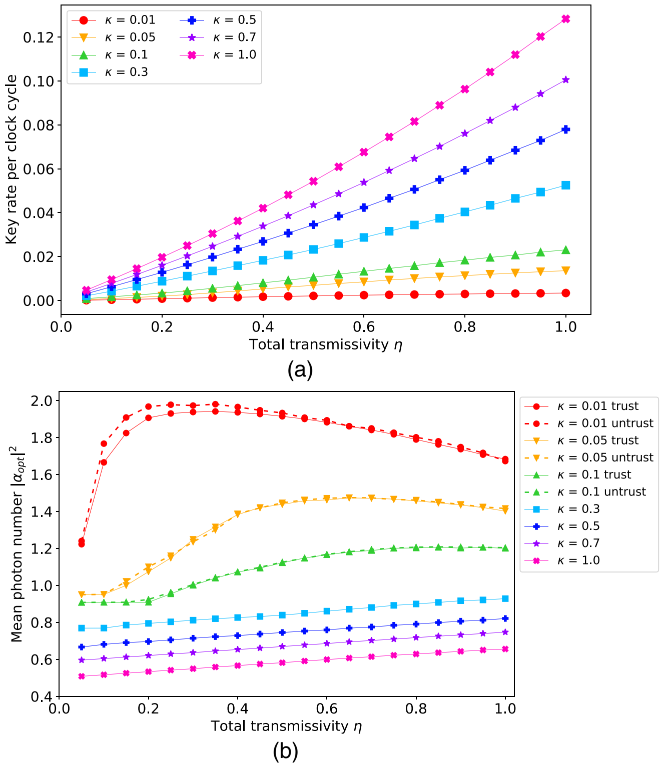
To simulate our statistics when dark counts are present, we generate the outcome probabilities with Bob's classically postprocessed POVM described in Sec. III C and Appendix A, which is associated with a dark-count probability, p_d, for each detector and at each detection time window.

If dark counts are assumed to be trusted in the sense that they are not in Eve's control, we use the classically postprocessed flag-state POVM $\{\widetilde{P}_k\}$ as the constraint matrices in the optimization problem (39) to calculate the privacy amplification term. This approach guarantees the optimization problem to be feasible since measurement probabilities correspond directly to a quantum state in the simulation.

However, if we consider untrusted dark counts, that is, if we pessimistically attribute the effect of dark-count noise to Eve, the flag-state POVM of dark-count-free detectors is used as the optimization constraint matrices instead. Note that unlike the existence of a physical model for pulling out the equal detection efficiency into the channel, this approach is not covered by any physical equivalence model that allows one to outsource the dark counts to Eve. Therefore, it is possible that no quantum states could have led to the classically postprocessed statistics if the measurement is assumed to be dark count free. In that case, the optimization problem becomes infeasible due to unphysical constraints. This is what we encounter in some parameter regime of our calculation, as we will point out in the next section.

VI. KEY RATES

Before diving into our main results, we start by stating the parameters used throughout this section. We set Bob's flag-state photon number cutoff to be $N_B = 4$ so that the PA term can be computed within a reasonable amount of time. The maximum number of terms kept in the PA summation in Eq. (38) is set to be $N_A = 3$ since we observe that the key rate in the low-loss regime does not improve even if we keep more than three terms. Furthermore, we set the dark-count probability to be $p_d = 8.5 \times 10^{-7}$ and the error-correction efficiency to be $f_{\text{EC}} = 1.22$ as quoted in Ref. [32].



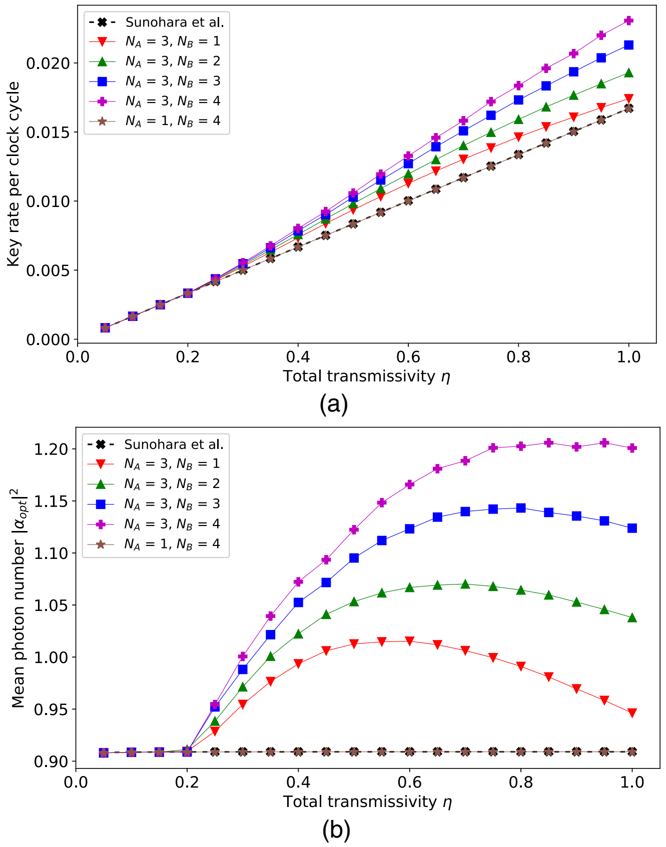
(a)

(b)

FIG. 3. (a) Our optimal lower bounds and (b) the corresponding mean photon numbers for secure key rates per clock cycle for both trusted (solid lines) and untrusted dark counts (dotted lines) vs total transmissivity η. For clarity, we omit labeling the lines for trusted and untrusted dark counts in the cases where the two lines are indistinguishable visually in the figure despite not being exactly the same.

In Fig. 3(a), we present lower bounds for the secure key rates per clock cycle corresponding to different values of the phase-modulator transmissivity κ and the total transmissivity η in the two scenarios with trusted and untrusted dark counts. The total transmissivity η captures both the transmission efficiency of the loss-only channel and the detection efficiency of Bob's detectors. We obtain these bounds by maximizing the lower bounds for key rates over the mean photon number $|\alpha|^2$ as specified in Sec. IV D. The optimal $|\alpha|^2$ for each point in Fig. 3(a) are shown in Fig. 3(b).

A careful reader will notice from Fig. 3(b) that the optimal mean photon numbers $|\alpha|^2$ follow a different trend for $\kappa \leqslant 0.1$ than those for $\kappa > 0.1$. One special feature appearing at $\kappa = 0.05$ and 0.1 is that the optimal $|\alpha|^2$ stays almost constant until the total transmissivity η reaches 0.1 and 0.2 where it suddenly increases. This sudden increase happens when the PA terms for $\widetilde{n} > 1$ in Eq. (38) turn strictly positive from zero, which is confirmed in Fig. 4. This figure shows that for fixed parameters $\kappa = 0.1$ and $N_B = 4$, the optimal key rates and $|\alpha|^2$ of the two tagged photon-number cutoffs $N_A = 1$ and 3 overlap when $\eta \leqslant 0.2$ meaning that the PA terms for $\widetilde{n} > 1$ are zero since keeping these terms gives no advantage compared with keeping only the $\widetilde{n} = 1$ term. This can be understood as a combination of the PNS and the unam-



(a)

(b)

FIG. 4. (a) Our optimal lower bounds and (b) the corresponding mean photon numbers for secure key rates per clock cycle evaluated at $\kappa = 0.1$ with trusted dark counts vs total transmissivity η. The results are produced using different tagged and flag-state photon number cutoffs, N_A and N_B. The optimal key rates and mean photon numbers of Ref. [6] appear as the black dotted line which overlaps with our key rates for $N_A = 1$ and $N_B = 4$.

biguous state discrimination (USD) [33] attacks, rendering the multiphoton signals completely known to Eve in the high-loss regime. For $\eta > 0.2$, the optimal key rates and $|\alpha|^2$ for $N_A = 3$ exceed those of $N_A = 1$, which indicate strict positivity of the PA terms for multiphoton signals. Back to Fig. 3(b), the reason why the sudden increase in the optimal $|\alpha|^2$ appears at a smaller η for smaller κ is that the orthogonality of the signal states reduces with κ, so a successful USD-type attack on the multiphoton signals will have to introduce more loss. For larger values of κ ($\kappa \gtrsim 0.3$), the domain with a significant increase in optimal mean photon number vanishes.

Another special feature about the optimal $|\alpha|^2$ that appears in Fig. 3(b) for $\kappa > 0.1$ is their nonmonotonic behavior in η, especially their decrease toward $\eta = 1$. This behavior is caused by the flag-state photon number cutoff N_B being too small. As Fig. 4(b) suggests, the nonmonotonicity in the plot of the optimal $|\alpha|^2$ against η tends to vanish as the cutoff N_B increases. The reason is that most of the photons in the multiphoton signals get transmitted as η approaches 1, so a small photon number cutoff N_B for the flag-state squashing model will assume Eve to measure all the signal components corresponding to photon number larger than N_B, a significant proportion of the signal, thereby losing a large part of the private information carried by the multiphoton signals. As the cutoff N_B decreases, less of this private information can be preserved. As a result, the optimal $|\alpha|^2$ decreases with N_B in order to put more weight on the PA terms for small $\tilde{n}$. The two features above mark the division in the key rate behaviors of the two parameter regimes $\kappa \lesssim 0.1$ and $\kappa \gtrsim 0.1$.

As a bonus observation, Fig. 4 shows that the lower bound for the secure key rate increases for larger flag-state photon number cutoff N_B, which corresponds to Eve measuring Bob's signals less frequently since a weak coherent signal has exponentially decreasing weight in larger photon number subspaces. The figure also confirms that the advantage of our analysis compared with the one in Ref. [6] appears only if we set the tagging cutoff to $N_A > 1$. We did not use larger cutoff N_B since the computational time for key rates using $N_B \geqslant 5$ will be too long.

Let us expand on the infeasibility issue with untrusted dark counts mentioned in Sec. V B. In the high-loss regime where the total transmissivity $\eta \leqslant 0.2$, the optimization problem for some parameters becomes infeasible, meaning that no physical states can satisfy the constraints that are imposed by observed statistics. This is a somehow surprising observation since many previous security analyses (e.g., Refs. [5,6,10,34]) assume dark counts to be untrusted but did not encounter any issue with infeasible constraints. Most of these analyses use coarse-grained statistics (e.g., bit/phase error rate) to bound Eve's knowledge. However, the use of refined statistics in our optimization constraints poses more stringent conditions on the feasible set, which makes it less robust against infeasibility issues. Therefore, at least when infeasibility is detected, we cannot outsource the dark counts simulated by a classical noise model entirely to Eve as previous literature did. In the case of having infeasible data, we allow the numerical solver to relax the satisfiability of constraints in the sense that we are enlarging the search set to the degree where it is feasible. Because of large constraint violations and a minimization over an enlarged search set, we expect the key rate lower bound obtained by this method to be much lower than the true value. As for the feasible cases, Fig. 3(a) shows that turning dark counts from untrusted to trusted increases the key rates. In the remaining of this section, if we make statements about the key rates without mentioning whether dark counts are trusted or untrusted, then the statement applies to both cases.

In the design view of a QKD security analysis, the goal is to optimize over all parameters and find the optimal setting of the experimental setup. Here, we seek the optimal asymmetric transmission parameter κ and the corresponding optimal signal intensity $|\alpha|^2$ that gives the highest key rate at different total transmissivity η. We see that with smaller values of κ, the key rates are lower in Fig. 3(a) because Alice would need to send more photons [as one can see from Fig. 3(b)] in order to maintain an adequate proportion of middle-click detection events, which allow Bob to infer the relative phase $\phi_x - \phi_B$. Therefore, one should always aim at reducing the loss at the phase modulator (i.e., increasing κ) in order to increase the overall key rate.

To elaborate more on the optimality of the intensities in Fig. 3(b), we point out the two competing factors for using more photons in the signal. First, sending higher intensity signals causes more photons to pass through Eve's

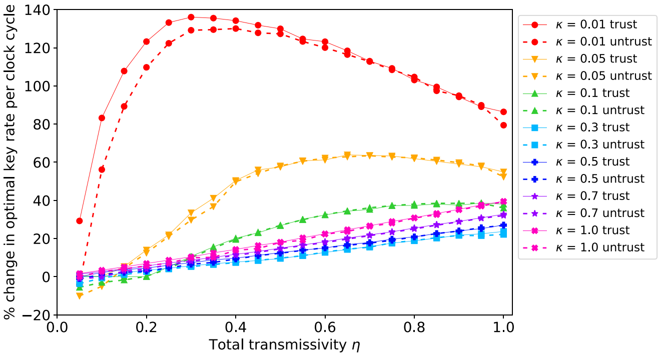


FIG. 5. Percentage change in key rates comparing our optimal lower bounds for key rates with Ref. [6]'s optimal key rates vs total transmissivity η. We label the changes for trusted (untrusted) dark counts with solid (dotted) lines. A positive change means that our key rate is higher.

domain, which allows her to gain more information about the signal, thereby reducing the key rate. Second, as more information can be transmitted from Alice to Bob via multiphoton signals, the key rate may increase if the cost of error correction increases less than the information gain by Eve.

These two factors pull the key rate into opposite directions, so there is an optimal point for the key rate to be maximized, of which the corresponding optimal mean photon number is shown in Fig. 3(b). These values appear to be higher than the optimal values for the key rates in Ref. [6]. This indicates that some multiphoton signals carry useful information from Alice to Bob of which Eve does not possess full knowledge and hence favor signals with higher intensity.

At this point, we would like to compare our results with previous results in Refs. [5,6], which both contain valid security proofs that make use of the single-photon components only. Note that although the technical analysis of Ref. [5] is correct, the conclusion that the key rate of the unbalanced BB84 protocol will be overestimated if one blindly uses the security analysis of a balanced protocol is not. While Ref. [5] has shown that the key rate for unbalanced signals is lower than that for balanced ones, the authors of Ref. [6] correctly point out that the drop in key rate is due to a smaller success rate of the unbalanced protocol, followed by the same key reduction during privacy amplification as for a balanced protocol. So in effect, during the operation of an unbalanced protocol, the use of privacy amplification terms from a balanced BB84 protocol still gives valid secret key rates. Therefore, it is incorrect for Ref. [5] to conclude that the drop in secure key rates for the unbalanced cases is due to the application of a new security analysis. Since Ref. [6] provides a known analytical key rate of this scenario, we use that result as the baseline of our investigations to show that in fact the secret key rate is underestimated by this security analysis and thus less privacy amplification is required in this situation.

We compare our key rates with Ref. [6]'s in Fig. 5, which shows that our analysis provides higher key rates for total transmissivity $\eta > 0.1$ (< 10 dB), especially for small κ values. Our method shows advantage in low-loss cases because the PA components from the multiphoton part of Alice's signals are larger in the low-loss regime, which are pessimistically set to zero in Ref. [6]. This can be understood as Eve does not learn too much of the multiphoton signals, thereby allowing more information to reach Bob.

When the total transmissivity satisfies $\eta \leqslant 0.2$, we encounter the issue with infeasible constraints with untrusted dark counts. We recover approximately the same key rates in Ref. [6] for most cases, but some of our lower bounds for the key rates (obtained from maximizing the dual SDP problem) in the untrusted noise scenario appear to be slightly lower than Ref. [6]'s. To understand the gaps between our key rate upper bounds (which are on par with Ref. [6]'s key rates) and lower bounds (see Sec. IV D for the meaning of the two bounds), we recall that our way of getting around the infeasibility issue with untrusted noise is to relax the required precision for the constraints to be satisfied in the numerical solver. The first-step suboptimal solution to the relaxed problem will naturally suffer from stronger constraint violations which lead to a lower dual suboptimal solution [16].

Notice that when the asymmetric loss parameter reaches $\kappa = 0.3$, the percentage increase of our key rate relative to Ref. [6]'s is the least compared to other values of κ. This phenomenon is also observed when we make the following choices of parameters: flag-state photon cutoff $N_B \in \{1, 2, 3, 4\}$, dark-count probability $p_d \in \{0, 10^{-5}, 10^{-4}\}$, and total transmissivity $\eta = 1$. As our numerical data suggest, the ratio between the optimal values of the privacy amplification terms attributed to Alice sending out one-photon and two-photon signals,

$$r_{21} = \frac{\min_{\rho_{AB}^2 \in \mathbf{S}_2} D(\mathcal{G}(\rho_{AB}^2)||\mathcal{Z}(\mathcal{G}(\rho_{AB}^2)))}{\min_{\rho_{AB}^1 \in \mathbf{S}_1} D(\mathcal{G}(\rho_{AB}^1)||\mathcal{Z}(\mathcal{G}(\rho_{AB}^1)))}, \tag{40}$$

reaches its smallest value when $\kappa \approx 0.3$. This can be interpreted as the amount of private information carried by two-photon signals relative to the amount carried by one-photon signals is the least when $\kappa \approx 0.3$, which corresponds to the points with the least key rate improvement.

As a remark, the optimal signal intensities $|\widetilde{\alpha}_{\rm opt}|^2$ for Ref. [6]'s optimal key rates (corresponding to Eq. (6) in Ref. [6]), which we compare with in Fig. 5, are slowly decreasing as η increases. They satisfy $|\widetilde{\alpha}_{\rm opt}|^2 \leqslant \min\{1, |\alpha_{\rm opt}|^2\}$, where $|\alpha_{\rm opt}|^2$ is the corresponding optimal intensity of our analysis as plotted in Fig. 3(b). This means that Ref. [6]'s optimal signal intensity is always smaller than our optimal intensity $|\alpha_{\rm opt}|^2$. It is also true that Ref. [6]'s optimal intensity increases as κ reduces for all tested values of η.

In the postprocessing view, the goal is to determine the amount of key reduction from privacy amplification that guarantees a secure final key for a given set of experimental parameters. Particularly in the case where the attenuation of the laser has already been set to Ref. [6]'s optimal intensity for a chosen set of parameters, we compare the privacy amplification term from our analysis with the one from Ref. [6]. To see this, we first show in Fig. 6 that our method still gives higher key rates than Ref. [6] in the low-loss regime ($\eta > 0.15$) even when our signal intensities are set to Ref. [6]'s. We then make the connection between this result and the difference in pri-

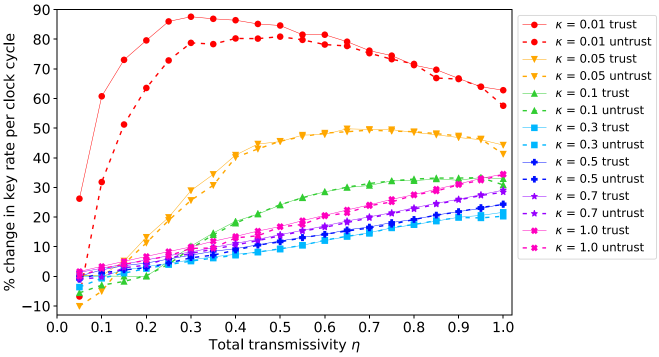


FIG. 6. Percentage change in key rates comparing our lower bounds for key rates per clock cycle evaluated at Ref. [6]'s optimal $\widetilde{\alpha}_{\mathrm{opt}}$ with Ref. [6]'s optimal key rates vs total transmissivity η. We label the changes for trusted (untrusted) dark counts with solid (dotted) lines. A positive change means that our key rate is higher.

vacy amplification with two observations: (1) The probability of passing postselection p_{pass} is equal for both methods and (2) the costs of error correction are approximately equal when the same signal intensity is used in both approaches. It follows that the difference in key rates translates to the difference in the privacy amplification terms in the key rate formula. Thus, our method requires less key reduction from privacy amplification compared to Ref. [6] for low-loss scenarios. This allows us to extract more secret keys out of these unbalanced protocols than previously thought.

We now turn to study the effect of trusted loss on the key rates. Previously, we assume that the quantum channel contributes completely to the total loss. However, if we know that a certain part of the total loss is caused by some trusted components (e.g., Bob's detectors), the key rate can be improved since the channel loss is effectively smaller. The key rate improvement has already been shown in both active and passive BB84 protocol [17], where the detection efficiency of the receiver's detectors is assumed to be beyond Eve's control. We will present a similar behavior of the key rates of this protocol under different trusted loss conditions.

We fix the total transmissivity to be $\eta = 0.1$ and assume dark counts are to be trusted, and then we vary the detection efficiency of Bob's trusted detectors η_{det}. Indeed, Fig. 7(a) shows that the lower bound of our optimal key rate increases with the proportion of the trusted loss component coming from Bob's detectors to the total loss, which takes the form $\frac{1-\eta_{\mathrm{det}}}{1-\eta}$. The optimal mean photon numbers corresponding to the optimal key rates are displayed in Fig. 7(b).

To summarize this section, we report a significant gain in key rates in the low-loss regime (< 10 dB) with our analysis. To be precise, with our security analysis, higher key rates can be obtained when the signal intensities are set to our optimal and Ref. [6]'s optimal values. We emphasize that the reported improvement can be attained without any modification to the experimental setup. Lastly, we show that the key rates can be increased if we know that the detection inefficiency contributes a considerable amount to the total loss.

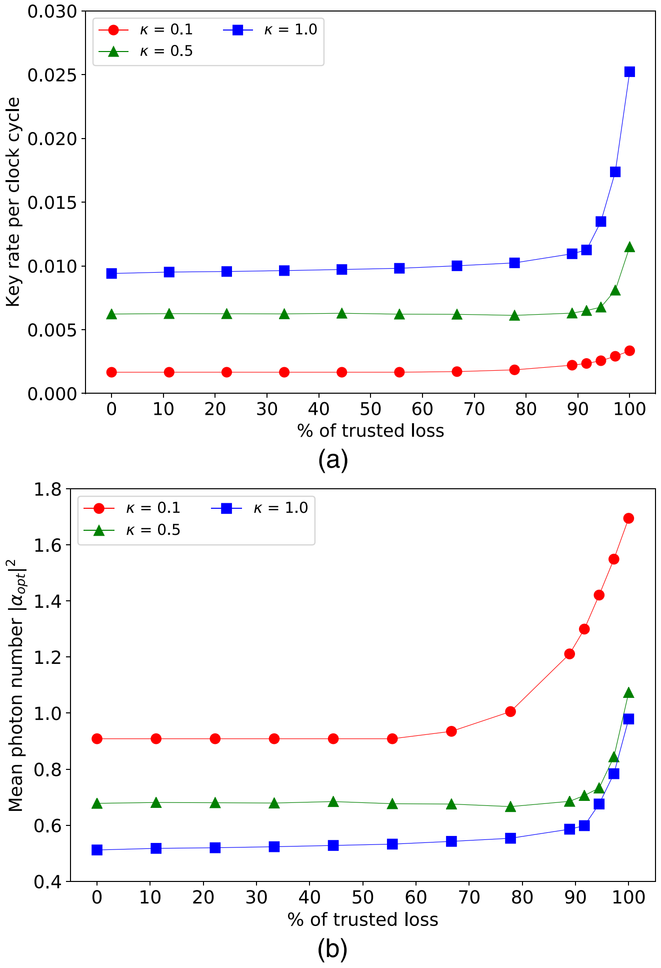


FIG. 7. Assuming trusted dark counts, (a) our lower bounds for key rates and (b) the mean photon numbers plotted against the proportion (in percentage) of the trusted loss coming from the detection inefficiency of Bob's detectors to a fixed total loss corresponding to total transmissivity $\eta = 0.1$.

VII. SUMMARY AND OUTLOOK

This work provides a numerical security proof for the unbalanced phase-encoded BB84 protocol. Using the flag-state squashing model [17], we are able to derive additional private information from the multiphoton components of the signal states. We compare our key rates with the key rates proved in Ref. [6] under the same simulation parameters and show that our analysis results in significantly higher key rates in the low-loss regime. In the design view, we find that a balanced protocol ($\kappa = 1$) gives a higher key rate than an unbalanced protocol so that a design cannot take advantage of an artificial induction of asymmetry. In the postprocessing view, our method requires less key reduction from privacy amplification compared to that of Ref. [6] for low-loss cases. We prove that our key rates are still better than Ref. [6]'s even when their optimal mean signal photon numbers are used. Hence, any experiments that are already implementing the optimal settings of Ref. [6] can profit from our higher key rates. We also explore the advantage of characterizing the receiver's detection inefficiency as a trusted loss, which is not allowed by the proof technique in Refs. [5,6]. Our results suggest that the key rate can be improved when the proportion of trusted loss due to detection inefficiency to the total loss is significant.

Let us conclude by pointing out some future directions of investigation: It is important to find a formal way of incorporating untrusted dark counts into the security analysis without leading to unphysical constraints. As mentioned in Sec. IV B, to extend our analysis to the use of a finite number of decoy states, one must consider the dependence among different feasible conditional state sets when handling the privacy amplification term. Finally, some of our proof techniques can be transferred to a finite-key analysis. It would be worth comparing the key rates from a finite-key analysis [35] with the asymptotic key rates reported here.

ACKNOWLEDGMENTS

The first author would like to thank Jie Lin and Shlok Nahar for reviewing his MATLAB code, which produces the results in this paper. We would also like to thank Ian George and Jie Lin for proofreading the Appendixes, and Adam Winick for the useful discussion on the numerical simulation of experimental statistics. The work has been performed at the Institute for Quantum Computing, University of Waterloo, which is supported by Industry Canada. The research has been supported by NSERC under the Discovery Grants Program, Grant No. 341495, and under the Collaborative Research and Development Program, Grant No. CRDP J 522308-17. Financial support for this work has been partially provided by Huawei Technologies Canada Co., Ltd. This research was enabled in part by the computational resources provided by WestGrid and Compute Canada.

APPENDIX A: DERIVATION OF THE LOWER BOUND FOR THE WEIGHT OF ($n \leqslant N_B$)-PHOTON SIGNAL SUBSPACE

We aim at lower bounding the weight of the ($n \leqslant N_B$)-photon signal subspace, $p(n \leqslant N_B)$, with Bob's observed statistics. In this Appendix, we use the cross-click probability to derive a lower bound for $p(n \leqslant N_B)$ in the following steps. The cross-click probability for any signal satisfies

$$\begin{aligned}
p(\mathrm{cc}) &= \sum_{n=0}^{N_B} p(n)p(\mathrm{cc}|n) + \sum_{n=N_B+1}^{\infty} p(n)p(\mathrm{cc}|n)\\
&\geqslant \sum_{n=0}^{N_B} p(n)p_{\min}(\mathrm{cc}|n) + \sum_{n=N_B+1}^{\infty} p(n)p_{\min}(\mathrm{cc}|n)\\
&\geqslant p(n \leqslant N_B)\, C^{\min}_{n\leqslant N_B} + [1 - p(n \leqslant N_B)]\, C^{\min}_{n>N_B}\\
&= C^{\min}_{n>N_B} - p(n \leqslant N_B)\big(C^{\min}_{n>N_B} - C^{\min}_{n\leqslant N_B}\big).
\end{aligned} \tag{A1}$$

In the second line, $p_{\min}(\mathrm{cc}|n)$ denotes the minimal cross-click probability given that Bob receives an n-photon signal. In the last two lines, we define $p(n \leqslant N_B) := \sum_{n=0}^{N_B} p(n)$, $C^{\min}_{n\leqslant N_B} := \min_{0\leqslant n\leqslant N_B} p_{\min}(\mathrm{cc}|n)$, and $C^{\min}_{n>N_B} := \min_{n>N_B} p_{\min}(\mathrm{cc}|n)$. If $p_{\min}(\mathrm{cc}|n)$ is monotonically increasing with n, then $C^{\min}_{n\leqslant N_B} = p_{\min}(\mathrm{cc}|0)$ and $C^{\min}_{n>N_B} = p_{\min}(\mathrm{cc}|N_B+1)$. If we also have strict inequality $C^{\min}_{n>N_B} > C^{\min}_{n\leqslant N_B}$, then we can turn the inequality in (A1) into the desired lower bound

$$p(n \leqslant N_B) \geqslant 1 - \frac{p(\mathrm{cc}) - p_{\min}(\mathrm{cc}|0)}{p_{\min}(\mathrm{cc}|N_B+1) - p_{\min}(\mathrm{cc}|0)} =: p^{\min}_{n\leqslant N_B}. \tag{A2}$$

We will show that the minimum cross-click probabilities indeed satisfy the monotonicity and the strict inequality conditions.

To obtain the minimum conditional probabilities $p_{\min}(\mathrm{cc}|0)$ and $p_{\min}(\mathrm{cc}|N_B+1)$, we start by considering the new POVM elements after classical postprocessing due to dark counts, as mentioned in Sec. III C, which are

$$P_0^{\phi_B} = (1-p_d)^6\, F_0^{\phi_B}\,, \tag{A3}$$

$$P_{t_1}^{\phi_B} = (1-p_d)^4\big\{F_{t_1}^{\phi_B} + [1-(1-p_d)^2]F_0^{\phi_B}\big\}, \tag{A4}$$

$$P_{t_3}^{\phi_B} = (1-p_d)^4\big\{F_{t_3}^{\phi_B} + [1-(1-p_d)^2]F_0^{\phi_B}\big\}, \tag{A5}$$

$$P_2^{\phi_B} = (1-p_d)^5\big(F_2^{\phi_B} + p_d\, F_0^{\phi_B}\big), \tag{A6}$$

$$P_5^{\phi_B} = (1-p_d)^5\big(F_5^{\phi_B} + p_d\, F_0^{\phi_B}\big), \tag{A7}$$

$$\begin{aligned}
P_{t_1,t_3}^{\phi_B} &= (1-p_d)^2\big\{F_{t_1,t_3}^{\phi_B} + [1-(1-p_d)^2]\big(F_{t_1}^{\phi_B} + F_{t_3}^{\phi_B}\big)\\
&\quad + [1-(1-p_d)^2]^2\, F_0^{\phi_B}\big\},
\end{aligned} \tag{A8}$$

$$P_{2,5}^{\phi_B} = (1-p_d)^4\big[F_{2,5}^{\phi_B} + p_d\big(F_2^{\phi_B} + F_5^{\phi_B}\big) + p_d^2\, F_0^{\phi_B}\big]. \tag{A9}$$

We first group the preprocessed POVM elements into two coarse-grained POVM elements: outside only (t_1, t_3, t_1+t_3) and inside only ("2", "5", "2" + "5"). Using Eqs. (19) and (20), the two elements can be expressed as

$$\begin{aligned}
F_{\mathrm{out}} &= \sum_{\phi_B\in\{0,\pi/2\}} \big(F_{t_1,t_3}^{\phi_B} + F_{t_1}^{\phi_B} + F_{t_3}^{\phi_B}\big)\\
&= \sum_{n=1}^{\infty}\sum_{i=0}^{n} \xi^i(1-\xi)^{n-i}|i, n-i\rangle\langle i, n-i|,
\end{aligned} \tag{A10}$$

$$\begin{aligned}
F_{\mathrm{in}} &= \sum_{\phi_B\in\{0,\pi/2\}} \big(F_{2,5}^{\phi_B} + F_2^{\phi_B} + F_5^{\phi_B}\big)\\
&= \sum_{n=1}^{\infty}\sum_{i=0}^{n} \xi^{n-i}(1-\xi)^i|i, n-i\rangle\langle i, n-i|.
\end{aligned} \tag{A11}$$

Similarly, the two coarse-grained postprocessed POVM elements can be found to be

$$\begin{aligned}
P_{\mathrm{out}} &= \sum_{\phi_B\in\{0,\pi/2\}} \big(P_{t_1,t_3}^{\phi_B} + P_{t_1}^{\phi_B} + P_{t_3}^{\phi_B}\big)\\
&= (1-p_d)^2\{F_{\mathrm{out}} + [1-(1-p_d)^4]F_0\},
\end{aligned} \tag{A12}$$

$$\begin{aligned}
P_{\mathrm{in}} &= \sum_{\phi_B\in\{0,\pi/2\}} \big(P_{2,5}^{\phi_B} + P_2^{\phi_B} + P_5^{\phi_B}\big)\\
&= (1-p_d)^4[F_{\mathrm{in}} + p_d(2-p_d)F_0],
\end{aligned} \tag{A13}$$

where the preprocessed no-click POVM element is $F_0 = |0,0\rangle\langle 0,0|$. Therefore, the postprocessed coarse-grained POVM elements for inside-only and outside-only clicks are diagonal in the two-mode Fock basis $\{|i, n-i\rangle : i = 0, \ldots, n\}$ for all $n \in \mathbb{N}$. The cross-click POVM element is

$$P_{\mathrm{cc}} = \mathbb{1}_B - \left(P_{\mathrm{out}} + P_{\mathrm{in}} + \sum_{\phi_B} P_0^{\phi_B}\right), \tag{A14}$$

which is also diagonal in the two-mode Fock basis. Since $P_{\rm cc}$ is already diagonal, it is straightforward to find $P_{\rm cc}$'s minimum eigenvalue restricted to the n-photon subspace, which corresponds to the minimum cross-click probability for any n-photon input states, analytically. For an eigenstate $|i, n-i\rangle$, the associated cross-click probability (the eigenvalue of $P_{\rm cc}$) can be found using Eqs. (A3)–(A14) as

$$\begin{aligned} p(\mathrm{cc}|\;|i,n-i\rangle) = 1 &- (1-p_d)^2\ \xi^i(1-\xi)^{n-i} \\ &- (1-p_d)^4\ \xi^{n-i}(1-\xi)^i \end{aligned} \tag{A15}$$

for $n \geqslant 1$, and for the vacuum state $|0, 0\rangle$ to be

$$p(\mathrm{cc}|0) = 1 - (1-p_d)^2[1 + p_d\ (1-p_d)^2(2-p_d)]$$

as stated in Eq. (28). Since there is only one eigenvalue in the vacuum subspace, we need not minimize the conditional probability [i.e., $p_{\min}(\mathrm{cc}|0) = p(\mathrm{cc}|0)$]. We exclude the case where the phase modulator has zero transmissivity ($\kappa = 0$), then $\xi = \frac{1}{1+\kappa} \in [\frac{1}{2}, 1)$, so the minimum cross-click probability for any ($n \geqslant 1$)-photon input state is

$$p_{\min}(\mathrm{cc}|n) = 1 - (1-p_d)^2\ \xi^n - (1-p_d)^4\ (1-\xi)^n,$$

as stated in Eq. (29), which is valid for all $n \geqslant 1$. Notice that $p_{\min}(\mathrm{cc}|n)$ is monotonically increasing with n, which agrees with our intuition that cross-click events are more likely with more incoming photons.

As we further restrict the dark-count probability to $p_d \in [0, 1)$, it is analytically straightforward to verify that for all $n \geqslant 1$ and $\xi \in [\frac{1}{2}, 1)$,

$$p(\mathrm{cc}|0) \leqslant p_{\min}(\mathrm{cc}|n) < p_{\min}(\mathrm{cc}|n+1), \tag{A16}$$

so the monotonicity and the strict inequality conditions for (A2) to hold are satisfied. The inequality (A2) is of the same form as (27) in Sec. IV A except that the observed cross-click probability in (27) is conditioned on Alice's signal choice x.

We now move on to prove that the lower bound in the inequality (A2) is tighter than the lower bound derived in Ref. [14] for no dark counts. We use the fact that

$$\frac{a-c}{b-c} \leqslant \frac{a}{b} \quad \text{, if } 0 \leqslant c \leqslant a \leqslant b, \tag{A17}$$

and all probabilities are positive to show that

$$\frac{p(\mathrm{cc}) - p(\mathrm{cc}|0)}{p_{\min}(\mathrm{cc}|N_B+1) - p(\mathrm{cc}|0)} \leqslant \frac{p(\mathrm{cc})}{p_{\min}(\mathrm{cc}|N_B+1)}\ . \tag{A18}$$

With (29), we can further show that

$$p_{\min}(\mathrm{cc}|N_B+1) \geqslant 1 - \xi^{N_B+1} - (1-\xi)^{N_B+1}\ . \tag{A19}$$

Thus, the lower bound in (A2) is larger than the lower bound derived in Ref. [14], which is the expression in (A2) for zero dark-count rate, as in

$$p(n \leqslant N_B) \geqslant p^{\min}_{n\leqslant N_B} \geqslant 1 - \frac{p(\mathrm{cc})}{1 - \xi^{N_B+1} - (1-\xi)^{N_B+1}}\ . \tag{A20}$$

The secure key rate should only reduce as we loosen the lower bound for the weight of the ($n \leqslant N_B$)-photon subspace since the flag-state squashing map can be more entanglement breaking and so Eve could gain more information from purification. As a result, we can use the dark-count-free lower bound blindly on Bob's measurement data to obtain a secure key rate even if the dark-count rate is assumed to be zero.

APPENDIX B: PROOF OF DECOMPOSING THE PRIVACY AMPLIFICATION TERM

In Sec. III B, Eqs. (8), (11), and (12) together describe the entangled pure state that Alice prepares to be

$$|\Psi\rangle_{AA_SA'} = \sum_x \sqrt{p_x}\ |x\rangle_A \otimes \sum_{\widetilde{n}=0}^{\infty} \sqrt{p_{\widetilde{n}}}\ |\widetilde{n}\rangle_{A_S} \otimes |s^x_{\widetilde{n}}\rangle_{A'},$$

where we simplify the notation here with $p_{\widetilde{n}} := p_{\widetilde{n}}(\frac{\alpha}{\sqrt{\xi}})$. Since the phase-randomized coherent signal states are block diagonal in total photon number basis in Eve's point of view, Eve can, without loss of generality, perform QND measurements to determine the total photon number in the signal states. This allows her to keep an extra classical register that tells her the total number of photons in the signal without degrading her eavesdropping power, as we will see below.

To see why allowing Eve to measure the total photon number in the signal state will not affect our security statement, we first consider the most general scenario where we do not assume anything about Eve's attack. By Stinespring's dilation theorem, the action of a quantum channel on the signal state can be described by an isometry $V_{A'\to BE}$ that takes Alice's signal system, A', to Bob's system, B, and Eve's purifying system, E, such that the pure state shared among all parties is

$$|\widetilde{\Psi}\rangle_{AA_SBE} = \sum_x \sqrt{p_x}\ |x\rangle_A \otimes \sum_{\widetilde{n}=0}^{\infty} \sqrt{p_{\widetilde{n}}}\ |\widetilde{n}\rangle_{A_S} \otimes V_{A'\to BE}\ \big|s^x_{\widetilde{n}}\big\rangle_{A'}\ .$$

Eve's general reduced state conditioned on Alice's measurement outcome x is

$$\rho^x_E = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\ \mathrm{Tr}_B\big(V_{A'\to BE}\ \big|s^x_{\widetilde{n}}\big\rangle\big\langle s^x_{\widetilde{n}}\big|\ V^\dagger_{A'\to BE}\big). \tag{B1}$$

In the alternative scenario, we assume that Eve performs the QND measurement and could perform adaptive attack according to her knowledge of the photon number. Let Eve's purifying system of the signal be E and the extra register for recording the photon number in Alice's signal be $\widetilde{E}$. Again by Stinespring's dilation theorem, one can describe the action of a quantum channel on the signal state by an isometry $V_{A'\to BE\widetilde{E}}$ which takes the form

$$V_{A'\to BE\widetilde{E}} = \sum_{\widetilde{n}=0}^{\infty} V^{\widetilde{n}}_{A'\to BE}\ \Pi^{A'}_{\widetilde{n}} \otimes |\widetilde{n}\rangle_{\widetilde{E}}, \tag{B2}$$

where $V^{\widetilde{n}}_{A'\to BE}$ is Eve's isometry for purifying Bob's quantum state given that she learns the total photon number $\widetilde{n}$ and $\Pi^{A'}_{\widetilde{n}}$ is a projector which projects onto the $\widetilde{n}$-total photon subspace of the signal system A'. The shared pure state among Alice, Bob, and Eve before any announcements is

$$|\Psi\rangle_{AA_SBE\widetilde{E}} = \sum_x \sqrt{p_x}\;|x\rangle_A \otimes \sum_{\widetilde{n}=0}^{\infty} \sqrt{p_{\widetilde{n}}}\;|\widetilde{n}\rangle_{A_S} \otimes V^{\widetilde{n}}_{A'\to BE}\;\big|s^x_{\widetilde{n}}\big\rangle_{A'} \otimes |\widetilde{n}\rangle_{\widetilde{E}} \tag{B3}$$

and Eve's reduced state conditioned on Alice's measurement outcome x is

$$\rho^x_{E\widetilde{E}} = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\,\mathrm{Tr}_B\big[V^{\widetilde{n}}_{A'\to BE}\;\big|s^x_{\widetilde{n}}\big\rangle\!\big\langle s^x_{\widetilde{n}}\big|\;\big(V^{\widetilde{n}}_{A'\to BE}\big)^{\dagger}\big] \otimes |\widetilde{n}\rangle\langle\widetilde{n}|_{\widetilde{E}}\;. \tag{B4}$$

If we further trace out Eve's register $\widetilde{E}$, her reduced state ρ^x_E clearly contains the general attack in (B1) where Eve performs the same purification (i.e., $V^{\widetilde{n}}_{A'\to BE} = V_{A'\to BE}$) for all $\widetilde{n} \in \mathbb{N}$. Therefore, the assumption that Eve can measure the photon number of the signal and the pure state shared by all parties to be (B3) will not affect the security statement of our proof.

To decompose the relative entropy in Eq. (31), we can assume the pure state shared by all parties to be (B3) as argued above. Hence, the state shared by Alice and Bob is

$$\rho_{AA_SB} = \sum_{x,y} \sqrt{p_x p_y}\;|x\rangle\langle y|_A \otimes \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\;|\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \Phi_{\widetilde{n}}\big(\big|s^x_{\widetilde{n}}\big\rangle\!\big\langle s^y_{\widetilde{n}}\big|\big), \tag{B5}$$

where the quantum channel between Alice and Bob is defined as $\Phi_{\widetilde{n}}(X) := \mathrm{Tr}_E[V^{\widetilde{n}}_{A'\to BE} X (V^{\widetilde{n}}_{A'\to BE})^{\dagger}]$ for any linear operator X that acts on the Hilbert space $\mathcal{H}_{A'}$. If we reorder the positions of the three registers in the tensor product and define the conditional state $\rho^{\widetilde{n}}_{AB} = \sum_{x,y} \sqrt{p_x p_y}\;|x\rangle\langle y|_A \otimes \Phi_{\widetilde{n}}(|s^x_{\widetilde{n}}\rangle\langle s^y_{\widetilde{n}}|)$, the state in (B5) can be expressed as

$$\rho_{AA_SB} = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\;|\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \rho^{\widetilde{n}}_{AB}\;. \tag{B6}$$

We will utilize this block-diagonal structure to decompose the relative entropy $D(\mathcal{G}(\rho_{AA_SB})||\mathcal{Z}(\mathcal{G}(\rho_{AA_SB})))$ in the following steps.

According to the definitions of $\mathcal{G}$ and $\mathcal{Z}$ maps stated in Eqs. (32)–(35), both maps act trivially on Alice's shield system A_S (i.e., apply $\mathbb{1}_{A_S}$ to the input state). Hence, the unnormalized states $\mathcal{G}(\rho_{AA_SB})$ and $\mathcal{Z}(\mathcal{G}(\rho_{AA_SB}))$ are also block diagonal as in

$$\mathcal{N}(\rho_{AA_SB}) = \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\;|\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \mathcal{N}\big(\rho^{\widetilde{n}}_{AB}\big) \tag{B7}$$

for $\mathcal{N}$ to be the substitute for the maps $\mathcal{G}$ and $\mathcal{Z}\circ\mathcal{G}$. Taking the matrix logarithm gives us

$$\log\mathcal{N}(\rho_{AA_SB}) = \sum_{\widetilde{n}=0}^{\infty} |\widetilde{n}\rangle\langle\widetilde{n}|_{A_S} \otimes \big[(\log p_{\widetilde{n}})\mathbb{1} + \log\mathcal{N}\big(\rho^{\widetilde{n}}_{AB}\big)\big]. \tag{B8}$$

By the definition of relative entropy, we decompose the PA term into

$$\begin{aligned}
&D(\mathcal{G}(\rho_{AA_SB})||\mathcal{Z}(\mathcal{G}(\rho_{AA_SB})))\\
&= \mathrm{Tr}\{\mathcal{G}(\rho_{AA_SB})[\log\mathcal{G}(\rho_{AA_SB}) - \log\mathcal{Z}(\mathcal{G}(\rho_{AA_SB}))]\}\\
&= \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\;\mathrm{Tr}\big\{\mathcal{G}\big(\rho^{\widetilde{n}}_{AB}\big)\big[\log\mathcal{G}\big(\rho^{\widetilde{n}}_{AB}\big) - \log\mathcal{Z}\big(\mathcal{G}\big(\rho^{\widetilde{n}}_{AB}\big)\big)\big]\big\}\\
&= \sum_{\widetilde{n}=0}^{\infty} p_{\widetilde{n}}\;D\big(\mathcal{G}\big(\rho^{\widetilde{n}}_{AB}\big)\big|\big|\mathcal{Z}\big(\mathcal{G}\big(\rho^{\widetilde{n}}_{AB}\big)\big)\big),
\end{aligned} \tag{B9}$$

which completes the proof.

APPENDIX C: JUSTIFICATIONS FOR SPEEDING UP NUMERICAL OPTIMIZATIONS

1. Reducing the number of variables

To speed up the optimization for the problem specified in (39), we make use of the structure of the flag-state squashed state. The joint state shared between Alice and Bob ρ_{AB} can be expressed as

$$\rho_{AB} = \sum_{i,j=1}^{d_A} \sum_{n,m=1}^{\infty} \rho^{n,m}_{i,j} E_{i,j} \otimes E_{n,m}\;\;, \tag{C1}$$

where $E_{i,j} = |i\rangle\langle j|$ with $\{|i\rangle\}$ being an orthonormal basis and $\rho^{n,m}_{i,j} \in \mathbb{C}\;\forall\; i, j, n, m$. Recall that the flag-state squashing map takes the form of (25) and since the dimension of the two-mode ($n \leqslant N_B$)-photon subspace is $\mathrm{Tr}(\Pi_{n\leqslant N_B}) = \frac{(N_B+1)(N_B+2)}{2}$, the joint state after squashing can be written as

$$\begin{aligned}
\widetilde{\rho}_{AB} &= (\mathbb{1}_A \otimes \Lambda)\rho_{AB}\\
&= \sum_{i,j=1}^{d_A} \sum_{n,m=1}^{\infty} \rho^{n,m}_{i,j} E_{i,j} \otimes \Lambda(E_{n,m})\\
&= \sum_{i,j=1}^{d_A} E_{i,j} \otimes \left(\sum_{n,m=1}^{\mathrm{Tr}(\Pi_{n\leqslant N_B})} \rho^{n,m}_{i,j} E_{n,m} + \sum_{k=1}^{M_B} c^k_{i,j} \widetilde{E}_{k,k} \right) && \text{(C2)}\\
&= (\mathbb{1}_A \otimes \Pi_{n\leqslant N_B})\rho_{AB}(\mathbb{1}_A \otimes \Pi_{n\leqslant N_B}) && \text{(C3)}\\
&\quad + \sum_{k=1}^{M_B} \left(\sum_{i=1}^{d_A} c^k_{i,i} E_{i,i} + \sum_{i<j}^{d_A} c^k_{i,j} E_{i,j} + (c^k_{i,j})^* E_{j,i} \right) \otimes \widetilde{E}_{k,k},
\end{aligned}$$

where we define $\widetilde{E}_{k,l} = E_{\mathrm{Tr}(\Pi_{n\leqslant N_B})+k,\;\mathrm{Tr}(\Pi_{n\leqslant N_B})+l}$, $c^k_{i,j} = \mathrm{Tr}[P_k\;(\sum_{n,m=\mathrm{Tr}(\Pi_{n\leqslant N_B})+1}^{\infty}\;\rho^{n,m}_{i,j} E_{n,m})]$, and M_B to be the number of POVM elements. Since ρ_{AB} is Hermitian, we also know that

$$\big(\rho^{n,m}_{i,j}\big)^* = \rho^{m,n}_{j,i}\text{ and }\big(c^k_{i,j}\big)^* = c^k_{j,i}\;. \tag{C4}$$

Therefore, we only have to optimize over $[d_A\;\mathrm{Tr}(\Pi_{n\leqslant N_B})]^2 + d_A^2 M_B$ real parameters instead of $[d_A(\mathrm{Tr}(\Pi_{n\leqslant N_B}) + M_B)]^2$ real parameters if we simply take the squashed state as a $d_A(\mathrm{Tr}(\Pi_{n\leqslant N_B}) + M_B)$-dimensional density matrix before imposing any optimization constraints. By reducing the number of parameters, we observe a significant speedup in the optimization (for $d_A = 4$ and $M_B = 28$).

2. Speedup in checking constraints

In the optimization problem (39), to impose each of the constraints requires explicit evaluation of the inner product between the updated squashed state ρ and each constraint matrix Γ_μ. As the squashed state and all the constraint matrices in (39) admit a block-diagonal structure, we only need to consider the matrix elements of ρ and $\{\Gamma_\mu\}$ that are contained in these blocks to calculate the inner product. We will show that by defining new optimization variables of smaller dimensions, the optimization problem (39) can be restructured so that each constraint can be checked faster. By doing so, the optimization problem can be solved more quickly.

Let Γ be a squashed constraint matrix, which is Hermitian and can be expressed in the squashed basis as

$$\Gamma = \sum_{i,j=1}^{d_A} E_{i,j} \otimes \left(\sum_{n,m=1}^{\mathrm{Tr}(\Pi_{n\leqslant N_B})} \Gamma_{i,j}^{n,m} E_{n,m} + \sum_{k,l=1}^{M_B} \widetilde{\Gamma}_{i,j}^{k,l} \widetilde{E}_{k,l} \right), \tag{C5}$$

where $\Gamma_{i,j}^{n,m}, \widetilde{\Gamma}_{i,j}^{k,l} \in \mathbb{C}$, which satisfy $(\Gamma_{i,j}^{n,m})^* = \Gamma_{j,i}^{m,n}$ and $(\widetilde{\Gamma}_{i,j}^{k,l})^* = \widetilde{\Gamma}_{j,i}^{l,k}\ \forall\ i, j, k, l, m, n$. We can split $\mathrm{Tr}(\Gamma\widetilde{\rho}_{AB})$ into three terms as in

$$\begin{aligned}\mathrm{Tr}(\Gamma\widetilde{\rho}_{AB}) &= \sum_{i,j=1}^{d_A} \left(\sum_{n,m=1}^{\mathrm{Tr}(\Pi_{n\leqslant N_B})} \Gamma_{i,j}^{n,m} \rho_{j,i}^{m,n} + \sum_{k=1}^{M_B} \widetilde{\Gamma}_{i,j}^{k,k} c_{j,i}^{k} \right) \\ &= \mathrm{Tr}(\Gamma \rho_{n\leqslant N_B}) + \langle \vec{\Gamma}_{\mathrm{flag}} | \vec{c}_{\mathrm{diag}} \rangle + 2\mathrm{Re}(\langle \vec{\Gamma}_{\mathrm{flag}} | \vec{c}_{\mathrm{off}} \rangle),\end{aligned} \tag{C6}$$

where we define $\rho_{n\leqslant N_B} = (\mathbb{1}_A \otimes \Pi_{n\leqslant N_B})\, \rho_{AB}\, (\mathbb{1}_A \otimes \Pi_{n\leqslant N_B})$, $|\vec{\Gamma}_{\mathrm{flag}}\rangle = \sum_{i,j=1}^{d_A} \sum_{k=1}^{M_B} \widetilde{\Gamma}_{i,j}^{k,k} |i\rangle \otimes |j\rangle \otimes |k\rangle$, $|\vec{c}_{\mathrm{diag}}\rangle = \sum_{i=1}^{d_A} \sum_{k=1}^{M_B} c_{i,i}^{k} |i\rangle \otimes |i\rangle \otimes |k\rangle$, and $|\vec{c}_{\mathrm{off}}\rangle = \sum_{i<j}^{d_A} \sum_{k=1}^{M_B} c_{i,j}^{k} |i\rangle \otimes |j\rangle \otimes |k\rangle$. The expression (C6) requires much fewer calculations in tracing the matrix product in the flag-state subspace (i.e., $\mathrm{span}\{\widetilde{E}_{k,l}\}$).

Define a function $\mathcal{R}(\sigma) = D(\mathcal{G}(\sigma)||\mathcal{Z}(\mathcal{G}(\sigma)))$ and an operator-valued function $\mathcal{M}$ which maps $\rho_{n\leqslant N_B}$, $|\vec{c}_{\mathrm{diag}}\rangle$, and $|\vec{c}_{\mathrm{off}}\rangle$ to the density matrix $\widetilde{\rho}_{AB}$ of the form in (C3) where the coefficients can be retrieved from $c_{i,i}^{k} = \langle i, i, k | \vec{c}_{\mathrm{diag}} \rangle$ and $c_{i,j}^{k} = \langle i, j, k | \vec{c}_{\mathrm{off}} \rangle$ with $|i, j, k\rangle := |i\rangle \otimes |j\rangle \otimes |k\rangle$. The convex optimization problem can be restructured into

$$\begin{aligned}&\text{minimize } \mathcal{R}(\mathcal{M}(\rho_{n\leqslant N_B}\ ,\ |\vec{c}_{\mathrm{diag}}\rangle,\ |\vec{c}_{\mathrm{off}}\rangle))\\ &\text{subject to}\\ &\quad \mathrm{Tr}(\Gamma_\mu\ \rho_{n\leqslant N_B}) + \langle \vec{\Gamma}_{\mu,\mathrm{flag}} | \vec{c}_{\mathrm{diag}} \rangle + 2\mathrm{Re}(\langle \vec{\Gamma}_{\mu,\mathrm{flag}} | \vec{c}_{\mathrm{off}} \rangle) = \gamma_\mu\ ,\\ &\quad \mathrm{Tr}(\widetilde{\Gamma}_\nu\ \rho_{n\leqslant N_B}) + \langle \vec{\widetilde{\Gamma}}_{\nu,\mathrm{flag}} | \vec{c}_{\mathrm{diag}} \rangle + 2\mathrm{Re}(\langle \vec{\widetilde{\Gamma}}_{\nu,\mathrm{flag}} | \vec{c}_{\mathrm{off}} \rangle) \geqslant \widetilde{\gamma}_\nu\ ,\\ &\quad \mathcal{M}(\rho_{n\leqslant N_B}\ ,\ |\vec{c}_{\mathrm{diag}}\rangle,\ |\vec{c}_{\mathrm{off}}\rangle) \geqslant 0,\end{aligned} \tag{C7}$$

where the free variables for the numerical optimization are $\rho_{n\leqslant N_B} \in \mathcal{D}(\mathbb{C}^{d_A \mathrm{Tr}(\Pi_{n\leqslant N_B})})$, $|\vec{c}_{\mathrm{diag}}\rangle \in \mathbb{R}^{d_A M_B}$, and $|\vec{c}_{\mathrm{off}}\rangle \in \mathbb{C}^{d_A(d_A-1)M_B/2}$.

Since the equality and inequality constraints [133 constraints in (39)] have to be checked for each run of the optimization, reducing the time and memory used in matrix multiplications of $\{\Gamma_\mu\}$ (and $\{\widetilde{\Gamma}_\nu\}$) with the squashed state $\widetilde{\rho}_{AB}$ substantially improves the runtime of the whole key rate calculation.

3. Speedup in evaluating $D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB})))$

Recall the definitions of the $\mathcal{G}$ and $\mathcal{Z}$ maps as stated in Eqs. (32)–(35). Using the form of the squashed shared state $\widetilde{\rho}_{AB}$ (which will be renamed as ρ_{AB} in the following) specified in Eq. (C2) with $i, j \in \{0, 1, 2, 3\}$ and $M_B = 28$, the state $\mathcal{G}(\rho_{AB})$ can be expanded into

$$\begin{aligned}\mathcal{G}(\rho_{AB}) = &\big[(|0\rangle\langle 0|_R \otimes E_{0,0}^{A}) \otimes \sigma_{0,0}\\ &+ (|0\rangle\langle 1|_R \otimes E_{0,2}^{A}) \otimes \sigma_{0,2}\\ &+ (|1\rangle\langle 0|_R \otimes E_{2,0}^{A}) \otimes \sigma_{2,0}\\ &+ (|1\rangle\langle 1|_R \otimes E_{2,2}^{A}) \otimes \sigma_{2,2}\big] \otimes |0\rangle\langle 0|_{\widetilde{B}}\\ &+ \big[(|0\rangle\langle 0|_R \otimes E_{1,1}^{A}) \otimes \sigma_{1,1}\\ &+ (|0\rangle\langle 1|_R \otimes E_{1,3}^{A}) \otimes \sigma_{1,3}\\ &+ (|1\rangle\langle 0|_R \otimes E_{3,1}^{A}) \otimes \sigma_{3,1}\\ &+ (|1\rangle\langle 1|_R \otimes E_{3,3}^{A}) \otimes \sigma_{3,3}\big] \otimes |1\rangle\langle 1|_{\widetilde{B}}\ ,\end{aligned} \tag{C8}$$

where $\sigma_{i,j} := \mathcal{F}_{\alpha(i)}^{B}(\sum_{n,m=1}^{\mathrm{Tr}(\Pi_{n\leqslant N_B})} \rho_{i,j}^{n,m} E_{n,m})\mathcal{F}_{\alpha(j)}^{B} + \mathcal{F}_{\alpha(i)}^{B}(\sum_{k=1}^{28} c_{i,j}^{k} \widetilde{E}_{k,k})\mathcal{F}_{\alpha(j)}^{B}$ with $\alpha(i) = i \bmod 2$. Applying the $\mathcal{Z}$ map to $\mathcal{G}(\rho_{AB})$ will give

$$\begin{aligned}\mathcal{Z}(\mathcal{G}(\rho_{AB})) = &\big[\big(|0\rangle\langle 0|_R \otimes E_{0,0}^{A}\big) \otimes \sigma_{0,0}\\ &+ \big(|1\rangle\langle 1|_R \otimes E_{2,2}^{A}\big) \otimes \sigma_{2,2}\big] \otimes |0\rangle\langle 0|_{\widetilde{B}}\\ &+ \big[\big(|0\rangle\langle 0|_R \otimes E_{1,1}^{A}\big) \otimes \sigma_{1,1}\\ &+ \big(|1\rangle\langle 1|_R \otimes E_{3,3}^{A}\big) \otimes \sigma_{3,3}\big] \otimes |1\rangle\langle 1|_{\widetilde{B}}\ .\end{aligned} \tag{C9}$$

Since Bob's basis announcement partitions $\mathcal{G}(\rho_{AB})$ into two orthogonal subspaces with the orthogonal projections and his quantum system B is further partitioned into two orthogonal subspaces [i.e., $(n \leqslant N_B)$-photon subspace and the flag-state subspace], $\mathcal{G}(\rho_{AB})$ as shown in Eq. (C8) can be broken down into four orthogonal subspaces.

Restricting to the image of map $\mathcal{G}$, matrices $\mathcal{G}(\rho_{AB})$ and $\mathcal{Z}(\mathcal{G}(\rho_{AB}))$ can be simplified to

$$\mathcal{G}(\rho_{AB}) = \begin{pmatrix} \sigma_{0,0} & \sigma_{0,2} & 0 & 0 \\ \sigma_{2,0} & \sigma_{2,2} & 0 & 0 \\ 0 & 0 & \sigma_{1,1} & \sigma_{1,3} \\ 0 & 0 & \sigma_{1,3} & \sigma_{3,3} \end{pmatrix}, \tag{C10}$$

$$\mathcal{Z}(\mathcal{G}(\rho_{AB})) = \begin{pmatrix} \sigma_{0,0} & 0 & 0 & 0 \\ 0 & \sigma_{2,2} & 0 & 0 \\ 0 & 0 & \sigma_{1,1} & 0 \\ 0 & 0 & 0 & \sigma_{3,3} \end{pmatrix}. \tag{C11}$$

Recall the definition of relative entropy, $D(\rho||\sigma) = \mathrm{Tr}(\rho\log\rho) - \mathrm{Tr}(\rho\log\sigma)$, which is finite if $\ker(\sigma) \subseteq \ker(\rho)$. We can restrict study to nonzero subspaces and express the objective function as in Eq. (C14) below:

$$\begin{aligned}&\mathrm{Tr}(\mathcal{G}(\rho_{AB})\log\mathcal{G}(\rho_{AB}))\\ &= \sum_{i=0}^{1} \big[\mathrm{Tr}\big(\tau_i^{n\leqslant N_B} \log \tau_i^{n\leqslant N_B}\big) + \mathrm{Tr}\big(\tau_i^{\mathrm{flag}} \log \tau_i^{\mathrm{flag}}\big)\big],\end{aligned} \tag{C12}$$

$$\begin{aligned}&\mathrm{Tr}(\mathcal{G}(\rho_{AB})\log\mathcal{Z}(\mathcal{G}(\rho_{AB})))\\ &= \sum_{i=0}^{1} \big[\mathrm{Tr}\big(\tau_i^{n\leqslant N_B} \log \mathcal{P}\big(\tau_i^{n\leqslant N_B}\big)\big) + \mathrm{Tr}\big(\tau_i^{\mathrm{flag}} \log \mathcal{P}\big(\tau_i^{\mathrm{flag}}\big)\big)\big],\end{aligned} \tag{C13}$$

$$D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB})))$$
$$= \sum_{i=0}^{1} \left[D\left(\tau_i^{n\leqslant N_B}||\mathcal{P}\left(\tau_i^{n\leqslant N_B}\right)\right) + D\left(\tau_i^{\text{flag}}||\mathcal{P}\left(\tau_i^{\text{flag}}\right)\right)\right], \quad \text{(C14)}$$

$$\tau_i^{\beta} := \begin{pmatrix} \sigma_{i,i}^{\beta} & \sigma_{i,i+2}^{\beta} \\ \sigma_{i+2,i}^{\beta} & \sigma_{i+2,i+2}^{\beta} \end{pmatrix}, \quad \mathcal{P}(\tau_i^{\beta}) := \begin{pmatrix} \sigma_{i,i}^{\beta} & 0 \\ 0 & \sigma_{i+2,i+2}^{\beta} \end{pmatrix}$$

with $\beta \in \{n \leqslant N_B, \text{flag}\}$, where we define the matrices $\sigma_{i,j}^{n\leqslant N_B} := \mathcal{F}_{\alpha(i)}^{B}(\sum_{n,m=1}^{\text{Tr}(\Pi_{n\leqslant N_B})} \rho_{i,j}^{n,m} E_{n,m})\mathcal{F}_{\alpha(j)}^{B}$ and $\sigma_{i,j}^{\text{flag}} := \mathcal{F}_{\alpha(i)}^{B}(\sum_{k=1}^{28} c_{i,j}^{k}\widetilde{E}_{k,k})\mathcal{F}_{\alpha(j)}^{B}$.

The objective function in (C14) only requires diagonalization and the logarithms of the smaller matrices τ_i^{β} and $\mathcal{P}(\tau_i^{\beta})$ for $i \in \{0, 1\}$ and $\beta \in \{n \leqslant N_B, \text{flag}\}$. Therefore, the expression in (C14) can be computed much more quickly than if we directly calculate the relative entropy with the full matrices $\mathcal{G}(\rho_{AB})$ and $\mathcal{Z}(\mathcal{G}(\rho_{AB}))$.

4. Speedup in evaluating the perturbed objective function

In the step of linearizing the convex optimization problem, the gradient of the objective function has to be evaluated at the suboptimal point obtained from the first step [16]. As pointed out in Sec. 3.2 of Ref. [16], the gradient is undefined if the matrix $\mathcal{G}(\rho_{AB})$ is not full rank. Besides, due to the finite numerical precision of a computer, the computed matrix $\mathcal{G}(\rho_{AB})$ may have negative eigenvalues for which the objective function is undefined. In these cases, we perform a perturbation on the matrix $\mathcal{G}(\rho_{AB})$ by applying a depolarizing channel which gives the perturbed map $\mathcal{G}_{\epsilon}(\rho_{AB})$, as defined in Ref. [16],

$$\begin{aligned}\mathcal{G}_{\epsilon}(\rho_{AB}) &:= (1-\epsilon)\mathcal{G}(\rho_{AB}) + \frac{\epsilon}{d'}\mathbb{1}_{d'} \\ &= (1-\epsilon)\mathcal{G}(\rho_{AB}) + \frac{\epsilon}{d'}\mathbb{1}|_{\text{Im}(\mathcal{G})} + \frac{\epsilon}{d'}\mathbb{1}|_{\ker(\mathcal{G})}\ ,\end{aligned} \quad \text{(C15)}$$

where $\epsilon > 0$ is the perturbation parameter and $d' = \dim(\mathcal{G}(\rho_{AB}))$. Applying the $\mathcal{Z}$ map to (C15) results in

$$\mathcal{Z}(\mathcal{G}_{\epsilon}(\rho_{AB})) = (1-\epsilon)\mathcal{Z}(\mathcal{G}(\rho_{AB})) + \frac{\epsilon}{d'}\mathbb{1}|_{\text{Im}(\mathcal{G})} + \frac{\epsilon}{d'}\mathbb{1}|_{\ker(\mathcal{G})}\ . \quad \text{(C16)}$$

The new objective function $D(\mathcal{G}_{\epsilon}(\rho_{AB})||\mathcal{Z}(\mathcal{G}_{\epsilon}(\rho_{AB})))$ is the relative entropy of the two perturbed matrices (C15) and (C16). We now show that the evaluation of the relative entropy can be restricted to the image of the map $\mathcal{G}$. We evaluate the matrix logarithms

$$\begin{aligned}\log\mathcal{G}_{\epsilon}(\rho_{AB}) &= \log\left[(1-\epsilon)\mathcal{G}(\rho_{AB}) + \frac{\epsilon}{d'}\mathbb{1}|_{\text{Im}(\mathcal{G})}\right] \\ &\quad + \log\left(\frac{\epsilon}{d'}\mathbb{1}|_{\ker(\mathcal{G})}\right), \qquad \text{(C17)} \\ \log\mathcal{Z}(\mathcal{G}_{\epsilon}(\rho_{AB})) &= \log\left[(1-\epsilon)\mathcal{Z}(\mathcal{G}(\rho_{AB})) + \frac{\epsilon}{d'}\mathbb{1}|_{\text{Im}(\mathcal{G})}\right] \\ &\quad + \log\left(\frac{\epsilon}{d'}\mathbb{1}|_{\ker(\mathcal{G})}\right). \qquad \text{(C18)}\end{aligned}$$

and define $\widetilde{\mathcal{G}}_{\epsilon}(\rho_{AB}) := \Pi_{\text{Im}(\mathcal{G})}\mathcal{G}_{\epsilon}(\rho_{AB})\Pi_{\text{Im}(\mathcal{G})}$ to obtain

$$\begin{aligned}&D(\mathcal{G}_{\epsilon}(\rho_{AB})||\mathcal{Z}(\mathcal{G}_{\epsilon}(\rho_{AB}))) \\ &= \text{Tr}\{\mathcal{G}_{\epsilon}(\rho_{AB})[\log\mathcal{G}_{\epsilon}(\rho_{AB}) - \log\mathcal{Z}(\mathcal{G}_{\epsilon}(\rho_{AB}))]\} \quad \text{(C19)} \\ &= \text{Tr}\{\widetilde{\mathcal{G}}_{\epsilon}(\rho_{AB})[\log\widetilde{\mathcal{G}}_{\epsilon}(\rho_{AB}) - \log\mathcal{Z}(\widetilde{\mathcal{G}}_{\epsilon}(\rho_{AB}))]\} \quad \text{(C20)} \\ &= D(\widetilde{\mathcal{G}}_{\epsilon}(\rho_{AB})||\mathcal{Z}(\widetilde{\mathcal{G}}_{\epsilon}(\rho_{AB}))). \quad \text{(C21)}\end{aligned}$$

The step going from (C19) to (C20) comes from the fact that Eq. (C17) minus (C18) results in the zero operator in the kernel of map $\mathcal{G}$. Now that we only have to consider the image of $\mathcal{G}$ in (C21), we can use the decomposition described in Eqn. (C14) but with the matrices τ_i^{β} and $\mathcal{P}(\tau_i^{\beta})$ replaced by $\widetilde{\tau}_i^{\beta}$ and $\mathcal{P}(\widetilde{\tau}_i^{\beta})$ respectively, which are defined as

$$\widetilde{\tau}_i^{\beta} := (1-\epsilon)\tau_i^{\beta} + \frac{\epsilon}{d'}(\mathbb{1}_{\beta} \oplus \mathbb{1}_{\beta}), \quad \text{(C22)}$$

$$\mathcal{P}(\widetilde{\tau}_i^{\beta}) := (1-\epsilon)\mathcal{P}(\tau_i^{\beta}) + \frac{\epsilon}{d'}(\mathbb{1}_{\beta} \oplus \mathbb{1}_{\beta}) \quad \text{(C23)}$$

with $\beta \in \{n \leqslant N_B, \text{flag}\}$. Since we can break down the evaluation of the perturbed objective function into calculations on restricted subspaces, the speedup described in Appendix C3 applies here.

[1] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[2] P. D. Townsend, Electron. Lett. **30**, 809 (1994).

[3] R. J. Hughes, G. G. Luther, G. L. Morgan, and C. Simmons, in *Coherence and Quantum Optics VII*, edited by J. H. Eberly, L. Mandel, and E. Wolf (Springer, Boston, 1996), pp. 103–111.

[4] H.-W. Li, Z.-Q. Yin, Z.-F. Han, W.-S. Bao, and G.-C. Guo, Quantum Info. Comput. **10**, 0771 (2010).

[5] A. Ferenczi, V. Narasimhachar, and N. Lütkenhaus, Phys. Rev. A **86**, 042327 (2012).

[6] S. Sunohara, K. Tamaki, and N. Imoto, arXiv:1302.1701.

[7] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[8] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[9] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[10] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[11] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[12] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[13] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, Phys. Rev. A **89**, 012325 (2014).

[14] V. Narasimhachar, Study of realistic devices for quantum key-distribution, MSc thesis, UWSpace, University of Waterloo, 2011, http://hdl.handle.net/10012/6348.

[15] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[16] A. Winick, N. Lütkenhaus, and P. J. Coles, Quantum **2**, 77 (2018).

[17] Y. Zhang, P. J. Coles, A. Winick, J. Lin, and N. Lütkenhaus, arXiv:2004.04383.

[18] H.-K. Lo, H. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2004).

[19] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[20] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[21] As we will point out in Sec. IV A, the number of POVM elements is related to the dimension of the flag-state subspace. If the two POVM elements are linearly dependent, they are essentially the same constraint for the convex optimization problem in (39) up to a scaling factor. Therefore, omitting either of the two elements will not affect the optimization result, but the flag-state subspace dimension will reduce by one. As for all numerical optimizations, the smaller the dimension of the problem, the shorter the runtime.

[22] M. Horodecki, P. W. Shor, and M. B. Ruskai, Rev. Math. Phys. **15**, 629 (2003).

[23] R. Renner, Nat. Phys. **3**, 645 (2007).

[24] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).

[25] R. Renner, arXiv:quant-ph/0512258 (2005).

[26] I. Devetak and A. Winter, Proc. R. Soc. London A **461**, 207 (2005).

[27] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Nat. Commun. **7**, 11712 (2016).

[28] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Phys. Rev. X **9**, 041064 (2019).

[29] H.-K. Lo, Quantum Inf. Comput. **5**, 413 (2005).

[30] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, UK, 2018).

[31] M. Frank and P. Wolfe, Nav. Res. Logist. Q. **3**, 95 (1956).

[32] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

[33] M. Dušek, M. Jahma, and N. Lütkenhaus, Phys. Rev. A **62**, 022306 (2000).

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

[35] I. George, J. Lin, and N. Lütkenhaus, arXiv:2004.11865.