Security proof of practical quantum key distribution with detection-efficiency mismatch

Yanbao Zhang,[1,2,3] Patrick J. Coles,[1,2,4] Adam Winick,[1] Jie Lin,[1,2] and Norbert Lütkenhaus[1,2]

[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

[2]*Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

[3]*NTT Basic Research Laboratories and NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[4]*Theoretical Division, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA*

(Received 16 April 2020; accepted 7 January 2021; published 25 January 2021)

Quantum key distribution (QKD) protocols with threshold detectors are driving high-performance QKD demonstrations. The corresponding security proofs usually assume that all physical detectors have the same detection efficiency. However, the efficiencies of the detectors used in practice might show a mismatch depending on the manufacturing and setup of these detectors. A mismatch can also be induced as the different spatial-temporal modes of an incoming signal might couple differently to a detector. Here we develop a method that allows to provide security proofs without the usual assumption. Our method can take the detection-efficiency mismatch into account without having to restrict the attack strategy of the adversary. Especially, we do not rely on any photon-number cutoff of incoming signals such that our security proof is directly applicable to practical situations. We illustrate our method for a receiver that is designed for polarization encoding and is sensitive to a number of spatial-temporal modes. In our detector model, the absence of quantum interference between any pair of spatial-temporal modes is assumed. For a QKD protocol with this detector model, we can perform a security proof with characterized efficiency mismatch and without photon-number cutoff assumption. Our method also shows that in the absence of efficiency mismatch in our detector model, the key rate increases if the loss due to detection inefficiency is assumed to be outside of the adversary's control, as compared to the view where for a security proof this loss is attributed to the action of the adversary.

DOI: 10.1103/PhysRevResearch.3.013076

I. INTRODUCTION

For practical quantum key distribution (QKD) [1] using photon-counting techniques (discrete variable QKD), information is usually encoded in optical signals that contain multiple photons. To decode the information, one measures the optical signals usually with threshold detectors which cannot tell apart the number of incoming photons. Security proofs of practical QKD protocols usually assume that all threshold detectors used have the same efficiency. Under this assumption, one can push the detection efficiency into the transmission channel, which is under the control of an adversary known as Eve. Thus the transmission loss and the inefficiencies of the detectors can be lumped together, and one can apply a security proof that applies to the new increased effective transmission loss followed by ideal threshold detectors with perfect efficiency [2].

In practice, however, it is not an easy job to build two detectors that have exactly the same efficiency. For example, the two detectors may be fabricated by different processes and so a mismatch between their efficiencies is induced. In the presence of efficiency mismatch, the different values for detection inefficiency cannot be lumped together and further treated as a single value for the loss over the transmission channel. Therefore existing security-proof techniques cannot be applied.

Even with a single detector, an efficiency mismatch can be induced by Eve. Suppose that the response of this detector to a photon depends on its degrees of freedom such as spatial mode, frequency, or arrival time. These degrees of freedom are not necessarily being used to encode information. If Eve can manipulate these degrees of freedom, then an effective efficiency mismatch is induced. When the induced mismatch is large enough, powerful attacks on QKD systems exist, as demonstrated in Refs. [3–8]. The intuition behind such attacks is as follows: The efficiency mismatch usually causes a specific outcome to be detected more frequently than the other outcomes in a chosen measurement basis; as a result, Eve can guess the outcomes correctly with a higher probability in the presence of efficiency mismatch than in the absence of efficiency mismatch. In typical experiments, the efficiency mismatch may not seem significant, but it still means that the security cannot be formally proven by existing techniques.

In this paper, we develop analytic tools that allow, subsequently, to prove with numerical methods the security in the presence of detection-efficiency mismatch. More precisely, we consider a setup designed for polarization encoding, where

each threshold detector used by the receiver Bob is sensitive to an incoming signal in a number of spatial-temporal modes. We assume a detector model where no quantum interference between any pair of spatial-temporal modes would take place as the incoming signal passes through the receiver or is being detected by a detector. However, the optical loss experienced by the signal can depend on its spatial-temporal mode. For the above detector model, the developed method can be applied given arbitrary characterized efficiency mismatch. To demonstrate our approach, we apply it to a Prepare&Measure BB84-QKD protocol [9]. Here we study the general case where the optical signals received by Bob may contain an unbounded number of photons such that their states live in an infinite-dimensional space. We can lower-bound the secret-key rate as a function of detection-efficiency mismatch and observed statistics. With our method, we can also study the individual effects of transmission loss and detection inefficiency on the secret-key rate. Our method is transferable to other QKD protocols. We note that Refs. [10–13] studied the security proof of the BB84-QKD protocol in the presence of efficiency mismatch *but* under the assumption that Bob receives no more than one photon at each round. However, this assumption cannot be justified in practical implementations of QKD where threshold detectors are being used.

We also remark that the spatial-temporal-mode-dependent efficiency-mismatch models studied by us (see Sec. II for details) are different from those mode-dependent mismatch models studied in the previous work [10]. As we assume the absence of quantum interference between any pair of spatial-temporal modes throughout the measurement process, the measurement operators are block-diagonal with respect to various photon-number subspaces, where in each photon-number subspace the number of photons in each spatial-temporal mode is specified. See our previous work [14] for the explicit expressions of these measurement operators. On the other hand, the previous work [10] studied the case that a quantum interference between a pair of auxiliary modes is possible, where the efficiency mismatch depends on these auxiliary modes. Therefore the detector model in Ref. [10] is more general than ours, albeit the security proof in Ref. [10] relies on a photon-number cutoff. Note that we believe that the interference between spatial-temporal modes will not play a significant role in a practical measurement setup. If we are wrong in this belief, our approach could be generalized to the more general detector model at the expense of more computational resources in our numerical key-rate evaluation.

The rest of the paper is structured as follows. In Sec. II we describe the basic setup for an optical BB84-QKD implementation with a special emphasis on the description of the spatial-temporal modes coupled to the detectors. Then we explain our method in Sec. III, where we also apply it to the described setup. In order to show the implication of our proof methods, we require a toy model that describes what observations we would expect in real experiments, which we do in Sec. IV. There we also show the secret-key rates that we obtain for setups that exhibit detection-efficiency mismatch. We summarize our findings in Sec. V. We note that all detectors considered in the rest of the paper are threshold detectors by default.

II. EXPERIMENTAL CONFIGURATION

The method that we develop in this article is about the treatment and analysis of the detector. Therefore, to lay out and illustrate the method we develop, it is sufficient to use the simple BB84 protocol [9], which we consider with an ideal single-photon source, but with threshold detectors monitoring full optical modes. Without loss of generality, we use the polarization-encoding language.

For our theoretical analysis, we use the entanglement-based formulation of Bennett, Brassard, and Mermin [15]. This approach has been later generalized for general QKD protocols to the source-replacement scheme [16]. This source-replacement scheme, in a thought-setup, realizes the source by preparing internally to the source a bi-partite entangled state. Measurements on one system effectively prepare the remaining system in the desired signal states with the prescribed probabilities. In the case of the BB84 protocol with an ideal single-photon source, the internal entangled state in the thought setup is the maximally entangled state

$$|\Phi\rangle_{\mathrm{AA}'} = \frac{1}{\sqrt{2}}(|H\rangle_{\mathrm{A}}|H\rangle_{\mathrm{A}'} + |V\rangle_{\mathrm{A}}|V\rangle_{\mathrm{A}'}), \tag{1}$$

where $|H\rangle$ and $|V\rangle$ are horizontally and vertically polarized single-photon states, respectively. System A' is prepared in the signal states of the BB84 protocol as Alice uniformly randomly selects to measure the system A in the horizontal/vertical (H/V) basis or the diagonal/anti-diagonal (D/A) basis. System A' enters the channel controlled by Eve and will emerge as system B at Bob's site. At that stage, the signal is not necessarily a single-photon signal, but can (due to Eve's action) be in any state of the optical modes supported by the detectors. For example, Eve might amplify the signal using an optical amplifier or replace the signals with multi-photon states at her discretion. Bob thus has to perform a measurement on the full optical modes, not on the single-photon signals. In our setup, he randomly selects to measure the signal in either the H/V basis or the D/A basis of the optical modes supported by his device. We call the above procedure of preparing, distributing and measuring signal states a *round*.

After a large number of rounds, with the data recordings that detail Alice's effective signal choices and Bob's measurement outcomes, Alice and Bob continue the QKD protocol using the usual steps of testing, sifting, key map, error correction, and privacy amplification to obtain secret keys. Our method can be easily generalized for other protocols that use, for example, weak coherent pulses as signal states, but the single-photon source example studied in this work is sufficient to demonstrate our method, which is about the detection side.

So let us turn our attention to Bob's detection: either the active- or passive-detection scheme, as depicted in Fig. 1, can be exploited. As the detectors used in each scheme are threshold detectors, each detector can respond to an incoming optical signal only in two different ways, click or no click. The detectors might respond to different modes (frequency, timing, etc).

As stated in the introduction, there are two scenarios where an detection-efficiency mismatch may exist. Let us start with the first one. Due to the fabrications or setups in practice,

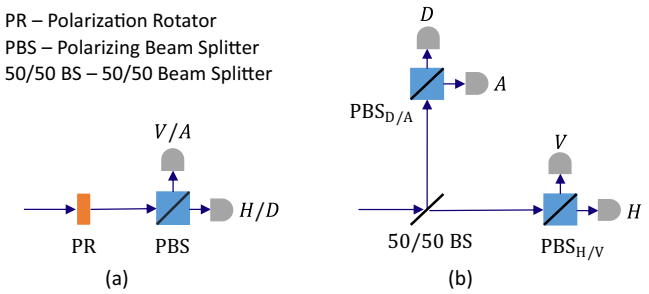

FIG. 1. Schematic of Bob's measurement device: (a) and (b) describe the active-detection and passive-detection schemes, respectively. To actively or passively select a measurement basis, a polarization rotator or a 50/50 beam splitter is used. Under each basis, a polarizing beam splitter and two detectors are used to measure the polarization state of an incoming optical signal. Each detector is labeled by the associated measurement outcome.

the two detectors shown in Fig. 1(a) for the active-detection scheme may have different efficiencies $\eta_{H/D}$ and $\eta_{V/A}$. Similarly, the four detectors in Fig. 1(b) for the passive-detection scheme may have efficiencies η_H, η_V, η_D, and η_A respectively. Here, the subscripts indicate the detectors used in a scheme. We call this kind of mismatch the spatial-temporal-mode-independent mismatch, in contrast to the following mismatch which depends additionally on the spatial-temporal modes chosen by Eve.

The second scenario is that of an active Eve. By manipulating the spatial-temporal mode of an optical signal, Eve can change the coupling of the signal with a detector, resulting in a change in the effective detection efficiency of the detector. Especially in free-space QKD it is possible for Eve to change the angle of an incoming signal [6–8] to influence the coupling of the signal with the active detection area of a detector, while for fiber-based signals simple time delays can be introduced [3] to exploit uneven aligned detection time windows. Therefore, in a setup with several detectors, the efficiencies of these detectors can not only differ from each other but also depend on the spatial-temporal modes coupled to the detectors, giving rise to the so-called spatial-temporal-mode-dependent mismatch. In this work, we analyze the security in both above scenarios.

Bob's detectors may respond to a large number of spatial-temporal modes. If the detection efficiencies related to these modes differ strongly from each other, it might become possible for Eve to control Bob's detection events thoroughly by sending the signals to the modes that couple particularly well only to a specific detector of Bob for which Eve desired to cause a detection event. For this attack to be possible in its extreme form, the number of modes must be equal to, or larger than, the number of detectors in the setup. For this reason, we choose the number of controllable modes to be equal to the number of detectors. In order to obtain visually simple illustrations of the secret-key rates, we choose mismatch models parametrized by two values for the efficiencies: a high value η_1 for one detector, and a lower value η_2 for the other detectors, as shown in Tables I and II. We emphasize that these mismatch models are considered just for ease of visual presentation, as the approach developed here can be exploited with an arbitrary mismatch model. To analyze the security of QKD systems, for example, in a certification process, the choice of the mismatch model and its parameters will need to be justified and characterized in practice.

TABLE I. Spatial-temporal-mode-dependent mismatch model in the active-detection scheme, where $0 \leqslant \eta_2 \leqslant \eta_1 \leqslant 1$. The efficiencies of the two detectors labeled in Fig. 1(a) are listed in a column, where each column corresponds to a spatial-temporal mode.

	Mode 1	Mode 2
Detector "H/D"	η_1	η_2
Detector "V/A"	η_2	η_1

III. KEY-RATE CALCULATION METHOD

A. Formulation of key-rate calculation as a convex-optimization problem

The asymptotic key rate certifiable against all collective attacks [17] is given by the difference between two terms, which are associated with privacy amplification (PA) and error correction (EC), respectively. The EC term depends only the the measurement statistics and can be calculated without any further information on the implementation of the QKD protocol. The main difficulty of the security proof relies on how to obtain a lower bound on the PA term. As shown in Refs. [18,19], a reliable numerical lower bound on the PA term can be provided by solving a convex-optimization problem. In the following, we will give a brief review of the theory behind that reformulation.

In a generic QKD protocol, the measurement statistics in an experiment are summarized as a probability distribution $p_{\mathrm{AB}}(x, y)$, where x and y are random variables corresponding to the events detected by Alice and Bob, respectively. The corresponding measurement operators are M_x^{A} and M_y^{B}. In addition, for the techniques shown in this paper, we will be able to provide from experimental observations lower bounds on the probability of at most k photons arriving at Bob. These bounds will be brought in as additional explicit constraints in the convex-optimization problem. To formulate the corresponding constraints, we introduce the projectors Π_k onto the photon-number subspace of Bob containing at most k photons, and the corresponding lower bound on its expectation value as b_k. Then, the calculation of the PA term, denoted by α, can be

TABLE II. Spatial-temporal-mode-dependent mismatch model in the passive-detection scheme, where $0 \leqslant \eta_2 \leqslant \eta_1 \leqslant 1$. The efficiencies of the four detectors labeled in Fig. 1(b) are listed in a column, where each column corresponds to a spatial-temporal mode.

	Mode 1	Mode 2	Mode 3	Mode 4
Detector "H"	η_1	η_2	η_2	η_2
Detector "V"	η_2	η_1	η_2	η_2
Detector "D"	η_2	η_2	η_1	η_2
Detector "A"	η_2	η_2	η_2	η_1

written as the convex-optimization problem [18,19]

$$\begin{aligned} \alpha := \min_{\rho_{\mathrm{AB}}} & D(\mathcal{G}(\rho_{\mathrm{AB}})||\mathcal{Z}(\mathcal{G}(\rho_{\mathrm{AB}}))) \\ \text{subject to} \quad & \rho_{\mathrm{AB}} \geqslant 0, \mathrm{Tr}(\rho_{\mathrm{AB}}) = 1 \\ & \mathrm{Tr}\big(\big(M_x^{\mathrm{A}} \otimes M_y^{\mathrm{B}}\big)\rho_{\mathrm{AB}}\big) = p_{\mathrm{AB}}(x,y) \\ & \mathrm{Tr}(\Pi_k \rho_{\mathrm{AB}}) \geqslant b_k \ . \end{aligned} \tag{2}$$

Here, $D(\sigma||\tau) := \mathrm{Tr}(\sigma \log_2 \sigma) - \mathrm{Tr}(\sigma \log_2 \tau)$ is the relative entropy, $\mathcal{G}$ is the post-selection map, and $\mathcal{Z}$ is the quantum channel describing the key map of the QKD protocol (see below for the details). In our applications we will later choose for $k \in \{1, 2\}$, or use even the constraints for both values of k. We remark that both the objective function and constraints are convex in the optimization variable ρ_{AB}.

Once we obtain a reliable lower bound β on the PA term α of Eq. (2) as $\beta \leqslant \alpha$ according to the numerical method developed in Ref. [19], the asymptotic key rate K per round is bounded by

$$K \geqslant K_{\mathrm{lb}} \doteq \beta - \mathrm{leak}_{\mathrm{obs}}^{\mathrm{EC}}, \tag{3}$$

where $\mathrm{leak}_{\mathrm{obs}}^{\mathrm{EC}}$ denotes the amount of information leaked to Eve per round of the protocol during error correction. This takes automatically into account any post-selection mechanism of the protocol, as any jointly discarded signals do not cause an error-correction cost. Likewise, the PA cost β automatically takes care of the same post-selection process, so that the total key rate K is counted as per round of the protocol. As we are discussing key rates in the asymptotic limit of a large number of exchanged signals, the reduction by any fraction of signals that is utilized to estimate the observed probability distribution $p_{AB}(x, y)$ of measurement results and other finite-size effects are negligible. Furthermore, the security proofs under collective and coherent attacks are equivalent in this limit [20], and hence our key-rate lower bound K_{lb} in principle holds for coherent attacks. We remark that the numerical method developed in Ref. [19] obtains a key-rate lower bound by the following two steps: First, by an iterative method, we find a near-optimal solution of the convex-optimization problem in Eq. (2) and thus an upper bound on the PA term α; second, we take advantage of the duality principle satisfied by convex optimization to obtain a reliable lower bound β on the PA term α. The key-rate lower bound K_{lb} obtained according to the numerical method developed in Ref. [19] is reliable in the sense that the lower bound K_{lb} is valid even considering the finite precision in floating-point representations. Moreover, the imprecision in function evaluations is estimated to be at the level of 10^{-8} according to the CVX package used by us for solving convex programs [21,22], although a rigorous analysis is currently missing and deserves further investigation in future work. The estimated function-evaluation imprecision is much smaller than the numerical key-rate lower bounds reported in Sec. IV, suggesting that our numerical key-rate lower bounds are reliable even considering the effect of function-evaluation imprecision.

The map $\mathcal{G}$ in the objective function of Eq. (2) describes the post-selection after Alice's and Bob's public announcements for sifting. For simplicity, we concentrate here on the case where to distill secret keys Alice and Bob keep only those signals where both measured in the H/V basis. We also note that for optical implementations, the announcements usually used for sifting are slightly more involved than the simple basis-dependent sifting of the BB84 protocol. The reason is that the potential presence of multiple photons in the incoming signals can cause several detectors to show detection events simultaneously. If Bob uses the active-detection scheme, the sifting announcement by Bob consists of the declaration whether he used the H/V basis measurement, and whether at least one detector fired. However, if Bob uses the passive-detection scheme, we have to decide what to do with events where we have multiple detections across the groups associated with different polarization bases (cross clicks), for example both the H and the D detector firings. Here we make the choice to keep only those events where either the H, the V, or both the H and V (denoted as HV event) detectors fire, while all other events (no clicks, clicks only in any of the D and the A detectors, or cross clicks) are being discarded. In order to achieve this goal, Alice publicly announces the basis choice where one of two bases is chosen uniformly randomly at each round, and Bob announces whether the desired events are observed. This corresponds to applying the post-selection map

$$\mathcal{G}(\rho_{\mathrm{AB}}) = G\rho_{\mathrm{AB}}G^{\dagger}, \tag{4}$$

where $G = \frac{1}{\sqrt{2}}\mathbb{1}^{\mathrm{A}} \otimes \sqrt{M_H^{\mathrm{B}} + M_V^{\mathrm{B}} + M_{HV}^{\mathrm{B}}}$ is a Kraus operator. Here, $\mathbb{1}^{\mathrm{A}}$ is the identity operator in the state space of Alice, and the positive-operator valued measure (POVM) elements M_H^{B}, M_V^{B}, and M_{HV}^{B} for Bob have been derived in Appendixes A and B of Ref. [14], with the remark that for the active-detection scheme we need to put the coefficient $1/2$ before each POVM element shown in Ref. [14] to account for Bob's probability of selecting each measurement basis.

After the public announcements and the corresponding post-selection step, Alice chooses a key map, which is represented by a quantum channel $\mathcal{Z}$. The key map is a function whose input is Alice's measurement outcome in the key-generation basis and whose output is a key value, 0 or 1. Suppose that we make a particular choice of key map here, namely that Alice's outcomes H and V are mapped to key values 0 and 1, respectively, and that the corresponding POVM elements M_H^{A} and M_V^{A} are projective (see Appendix). The application of the key map corresponds to the application of the quantum channel

$$\begin{aligned} \mathcal{Z}(\mathcal{G}(\rho_{\mathrm{AB}})) = & \big(M_H^{\mathrm{A}} \otimes \mathbb{1}^{\mathrm{B}}\big)\mathcal{G}(\rho_{\mathrm{AB}})\big(M_H^{\mathrm{A}} \otimes \mathbb{1}^{\mathrm{B}}\big) \\ & + \big(M_V^{\mathrm{A}} \otimes \mathbb{1}^{\mathrm{B}}\big)\mathcal{G}(\rho_{\mathrm{AB}})\big(M_V^{\mathrm{A}} \otimes \mathbb{1}^{\mathrm{B}}\big). \end{aligned} \tag{5}$$

Given the measurement statistics $p_{\mathrm{AB}}(x, y)$, the lower bounds b_k on the photon-number distribution, the post-selection map $\mathcal{G}$, and the key-map-realizing quantum channel $\mathcal{Z}$, in principle we can run numerical optimization to obtain a reliable lower bound of the minimization problem in Eq. (2). However, for the situation studied, the number of photons arriving at Bob is unbounded and so the dimension of the quantum state ρ_{AB} is infinite. For this reason we need to develop techniques that allow us to simplify the optimization problem such that a reliable key-rate lower bound can be numerically obtained by optimizing over only finite-dimensional

quantum states. These techniques are described in the next two subsections.

B. Simplification of the convex-optimization problem: flag-state squasher

Since Bob's measurement POVMs are block-diagonal with respect to the subspaces associated with total photon numbers across all modes [14], we can assume without loss of generality that Eve performs a quantum non-demolition (QND) measurement of the total photon number after her interaction with the signals, and before their arrivals at Bob's side. As a consequence, the state ρ_{AB} can be assumed, without loss of generality, to be block-diagonal with the same subspace structure, meaning that the state takes the form

$$\rho_{\mathrm{AB}} = \bigoplus_{n=0}^{\infty} p_n \rho_{\mathrm{AB}}^{(n)}. \tag{6}$$

The weight of each subspace carrying a total number of n photons is given by the corresponding probability p_n, and the corresponding normalized conditional state is denoted by $\rho_{\mathrm{AB}}^{(n)}$.

Considering the block-diagonal structure of the state and Bob's measurement POVMs, we can write

$$\begin{aligned} \rho_{\mathrm{AB}} &= p_{n\leqslant k}\rho_{\mathrm{AB}}^{(n\leqslant k)} \bigoplus (1-p_{n\leqslant k})\rho_{\mathrm{AB}}^{(n>k)}, \\ M_y^{\mathrm{B}} &= M_{y,n\leqslant k}^{\mathrm{B}} \bigoplus M_{y,n>k}^{\mathrm{B}}, \end{aligned} \tag{7}$$

where k is a free parameter chosen in the security proof and $p_{n\leqslant k}$ is the probability that no more than k photons arrive at Bob. The $(n \leqslant k)$-photon subspace is of finite dimension, which is compatible with the numerical key-rate optimization framework. On the other hand, the $(n > k)$-photon subspace is infinite dimensional, which is not directly suitable to be handled by our numerical method. To resolve this problem, we introduce the *flag-state squasher*. The general framework of squashing models that map large-dimensional state/measurement descriptions without loss of generality to lower-dimensional systems has been described in Refs. [23–25].

Theorem 1. **Flag-State Squasher** Suppose that we have a POVM with elements M_y, where $y \in \{1, \ldots, J\}$, such that each element can be written in a block-diagonal form $M_{y,n\leqslant k} \oplus M_{y,n>k}$, with an associated Hilbert space structure given by $\mathcal{H}_{n\leqslant k} \oplus \mathcal{H}_{n>k}$. Then there exists a completely positive trace preserving (CPTP) map Λ (referred to as a squashing map) from $\mathcal{H}_{n\leqslant k} \oplus \mathcal{H}_{n>k}$ to $\mathcal{H}_{n\leqslant k} \oplus \mathcal{H}_J$, where the dimension $dim(\mathcal{H}_J) = J$, such that $\mathrm{Tr}(\rho M_y) = \mathrm{Tr}(\Lambda(\rho)\tilde{M}_y)\ \ \forall \rho \in \mathcal{H}_{n\leqslant k} \oplus \mathcal{H}_{n>k}$ with

$$\tilde{M}_y = M_{y,n\leqslant k} \oplus |y\rangle\langle y| \ , \tag{8}$$

where the states $|y\rangle$ form an orthonormal basis of $\mathcal{H}_J$.

Proof. We need to show that the CPTP map Λ exists with the desired properties. This can be done by an explicit construction as indicated in Fig. 2. For this purpose, we consider a general input state given in block form $\rho = \begin{pmatrix} \rho_{\mathrm{ss}} & \rho_{\mathrm{sl}} \\ \rho_{\mathrm{ls}} & \rho_{\mathrm{ll}} \end{pmatrix}$, where index 's' refers to the small subspace $\mathcal{H}_{n\leqslant k}$ and index "l" to the large subspace $\mathcal{H}_{n>k}$. We can then describe the action of the squashing map Λ by its action onto an arbitrary input state

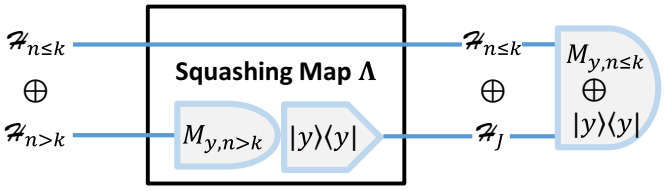

FIG. 2. Constructive description of the squashing map Λ for the flag-state squasher. Each line corresponds to a subspace of the input Hilbert space associated with the block-diagonal decomposition of the POVM elements M_y with $y \in \{1, \ldots, J\}$, as indicated on the left side.

of the above form as

$$\Lambda(\rho) = \begin{pmatrix} \rho_{\mathrm{ss}} & 0 \\ 0 & \sum_{y=1}^{J} (\mathrm{Tr}(\rho_{\mathrm{ll}} M_{y,n>k})\ |y\rangle\langle y|) \end{pmatrix}. \tag{9}$$

It is straightforward to see that the state $\Lambda(\rho)$ satisfies the properties $\mathrm{Tr}(\rho M_y) = \mathrm{Tr}(\Lambda(\rho)\tilde{M}_y)\ \ \forall y$ required by a flag-state squasher. ■

The large subspace $\mathcal{H}_{n>k}$, which in the case of Bob's measurement is infinite dimensional, is simply reduced to a smaller subspace $\mathcal{H}_J$ by performing the measurement $\{M_{y,n>k}, y = 1, \ldots, J\}$ on $\mathcal{H}_{n>k}$ and flagging the result y into an orthogonal register which replaces the original large subspace. This approach of creating squashing models to smaller Hilbert spaces relies only on the block-diagonal structure of the original POVM elements. As soon as that assumption is met, a flag-state squasher can be constructed. In this work, we apply Theorem 1 to Bob's states and measurements. As Bob's measurements are block-diagonal for an arbitrary choice of k [see Eq. (7)], we can freely choose which large photon-number subspace of Bob to be flagged. For this reason, we refer to the free parameter k as the *photon-number flag threshold*.

As in any case where a squashing map exists mapping the original measurement to an alternative measurement of a smaller dimension, we can assume that the squashing map is part of Eve's action. As a result, we overestimate Eve's power (see below for a detailed explanation), but as a trade-off we can now assume without further loss of generality that Bob receives signals in a reduced, finite-dimensional Hilbert space. So the key-rate optimization problem in Eq. (2) formulated with the squashed states of the form in Eq. (9) and POVM elements of the form in Eq. (8), which is a finite-dimensional convex-optimization problem, will provide a lower bound on the secret-key rate in the actual implementation. Note, however, that the virtual POVM element components $\tilde{M}_{y,n>k}^{\mathrm{B}} = |y\rangle\langle y|$ are projective and orthogonal. Therefore, when her QND measurement result of the total photon number is $n > k$ Eve could perform a strong attack by measuring the incoming signals from Alice with Bob's actual measurement $\{M_{y,n>k}^{\mathrm{B}} : y = 1, \ldots, J\}$ and then preparing/sending to Bob the flag state $|y'\rangle$ corresponding to her measurement result y'. This attack would deterministically trigger the same result y' when Bob performs the virtual measurement $\{\tilde{M}_{y,n>k}^{\mathrm{B}} : y = 1, \ldots, J\}$ according to the squashing map. Hence, by attributing the squashing map to Eve's action, Eve could

completely learn every result of Bob when $n > k$, and so we overestimate the power of Eve as compared with in the actual implementation. For this reason, the flag-state squasher must be accompanied by a constraint that limits the resulting state mostly to the $(n \leqslant k)$-photon subspace, which is given by the bound b_k in our optimization problem of Eq. (2).

Finally, we remark that without loss of generality the states ρ_{AB} and $\rho_{\mathrm{AB}}^{(n)}$ can be assumed to be real-valued. This is because all measurement POVM elements M_x^{A} and M_y^{B} of Alice and Bob can be represented by real-valued matrices and because the objective function to be minimized for bounding the key rate in Eq. (2) is a convex function of the state ρ_{AB}. For detailed proofs, see for example Sec. V C in Ref. [26]. We also emphasize that the block-diagonal structure and the real-matrix representation of the state ρ_{AB} apply to both the active- and passive-detection schemes. By using a real-matrix representation of ρ_{AB}, the number of free parameters in the key-rate optimization problem of Eq. (2) is reduced.

C. Constraints on photon-number distribution

To solve the convex-optimization problem in Eq. (2), we need make use of a flag-state squasher as introduced in theorem 1 where the small subspace will be chosen to be the incoming subspace containing at most $n = 1$ photon, or at most $n = 2$ photons. In order to obtain positive key rates, it will be necessary to show that the overlap of the incoming states with this subspace can be lower-bounded by some number b_k, $k = 1$ or 2. Following the numerical method developed in our previous study of entanglement verification with efficiency mismatch [14], we obtain such bounds directly from the experimentally observed measurement statistics $p_{\mathrm{AB}}(x, y)$. The intuition behind this approach is that higher photon numbers will necessarily lead to double clicks, cross clicks, and/or errors.

This way of using experimental observations to bound the photon-number distribution was first established in Ref. [2] and further refined in Ref. [27], and then extended to the case of inefficient detectors in Ref. [14]. Note that the theoretical approach is independent of the number of spatial-temporal modes that we use (in addition to the polarization degree of freedom). We demonstrate the results of our method here for the two-mode case (with the active-detection scheme) and for the four-mode case (with the passive-detection scheme).

Before explaining the method, we would like to point out that the two properties of the state ρ_{AB} discussed in the above subsection, i.e., the block-diagonal structure with respect to various photon-number subspaces and the real-number representation of the density matrix, will be used also in the optimization problems formulated in this subsection. The second property helps to reduce the number of free parameters in the optimization.

1. Active-detection case

As stated before, the intuition is that as an increasing number of photons are received by Bob, the probability of double clicks (clicks at both detectors) will increase and finally surpass the double-click probability observed in an experiment. Similar arguments hold for an effective error, which we define below. Thus we will show that the experimental observations allow us to put an upper bound on the probability that the signals received by Bob contain more than any given number of photons.

In order to make this intuition precise, we start by defining the double-click operator

$$F_{DC} = \tfrac{1}{2}\mathbb{1}^{\mathrm{A}} \otimes M_{HV}^{\mathrm{B}} + \tfrac{1}{2}\mathbb{1}^{\mathrm{A}} \otimes M_{DA}^{\mathrm{B}}, \tag{10}$$

and the effective-error operator

$$\begin{aligned} F_{EE} = {} & \tfrac{1}{2}M_H^{\mathrm{A}} \otimes \left(M_V^{\mathrm{B}} + \tfrac{1}{2}M_{HV}^{\mathrm{B}}\right) + \tfrac{1}{2}M_V^{\mathrm{A}} \otimes \left(M_H^{\mathrm{B}} + \tfrac{1}{2}M_{HV}^{\mathrm{B}}\right) \\ & + \tfrac{1}{2}M_D^{\mathrm{A}} \otimes \left(M_A^{\mathrm{B}} + \tfrac{1}{2}M_{DA}^{\mathrm{B}}\right) + \tfrac{1}{2}M_A^{\mathrm{A}} \otimes \left(M_D^{\mathrm{B}} + \tfrac{1}{2}M_{DA}^{\mathrm{B}}\right), \end{aligned} \tag{11}$$

where the prefactor $1/2$ at each term describes the probability to choose the corresponding measurement basis. The form of the effective-error operator is chosen according to the squashing model [23,24] for the active-detection scheme: the double-click events are mapped uniformly randomly in a post-processing step to either of the two single-click events associated with the chosen basis. In Eqs. (10) and (11), Alice's measurement operators are ideal measurement operators in the one-photon space (see Appendix), while Bob's measurement operators are described in Appendixes A and B of Ref. [14].

We formalize the above intuition by studying the following optimization problems

$$\begin{aligned} d_{n,\min} = {} & \min_{\rho_{\mathrm{AB}}^{(n)}} \mathrm{Tr}\left(\rho_{\mathrm{AB}}^{(n)} F_{DC}^{(n)}\right) \\ \text{subject to} \quad & \rho_{\mathrm{AB}}^{(n)} \geqslant 0 \\ & \mathrm{Tr}\left(\rho_{\mathrm{AB}}^{(n)}\right) = 1 \end{aligned} \tag{12}$$

and

$$\begin{aligned} e_{n,\min} = {} & \min_{\rho_{\mathrm{AB}}^{(n)}} \mathrm{Tr}\left(\rho_{\mathrm{AB}}^{(n)} F_{EE}^{(n)}\right) \\ \text{subject to} \quad & \rho_{\mathrm{AB}}^{(n)} \geqslant 0 \\ & \mathrm{Tr}\left(\rho_{\mathrm{AB}}^{(n)}\right) = 1\,. \end{aligned} \tag{13}$$

The operators $F_{DC}^{(n)}$ and $F_{EE}^{(n)}$ are projections of the operators F_{DC} and F_{EE} onto the n-photon subspace of Bob. We remark that the above optimizations are over all possible n-photon states $\rho_{\mathrm{AB}}^{(n)}$, while the optimization problems formulated in our previous study of entanglement verification with efficiency mismatch [14] run over only the states $\rho_{\mathrm{AB}}^{(n)}$ satisfying the positive-partial-transpose criterion [28,29].

The optimization problems described by Eqs. (12) and (13) have the form of semi-definite programs (SDPs). In order to solve them, we utilize the YALMIP [30] toolbox in MATLAB. From our calculations, we make the observation that the minimum double-click probability $d_{n,\min}$ is monotonically nondecreasing as the photon number n goes up. We therefore obtain the inequality

$$d_{n,\min} \geqslant d_{3,\min}, \quad \forall n \geqslant 3. \tag{14}$$

Moreover, we observed the inequality relations

$$e_{n,\min} \geqslant e_{3,\min}, \quad \forall n \geqslant 3, \tag{15}$$

and

$$e_{n,\min} \geqslant e_{\min} := \min\{e_{2,\min}, e_{3,\min}\}, \quad \forall n \geqslant 2. \tag{16}$$

We would like to point out that we did not go through the effort to prove the above inequalities with analytical methods,

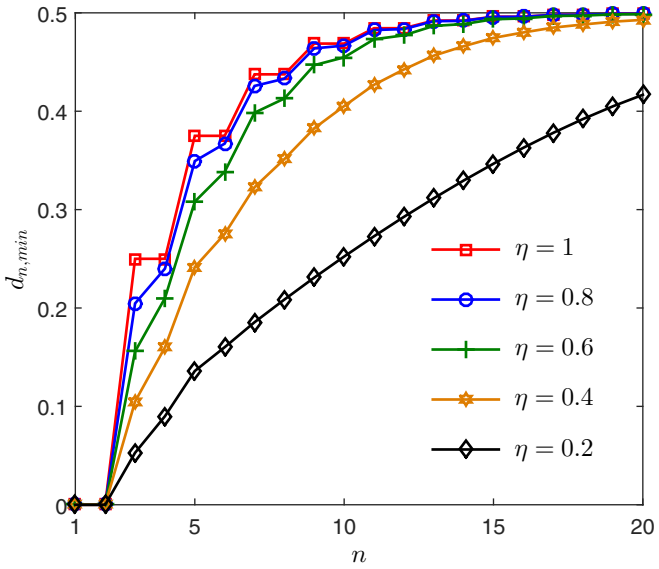

FIG. 3. The minimum double-click probability $d_{n,\min}$ vs. the photon number n received by Bob for the active-detection mismatch model of Table I with $\eta_1 = 1$ and $\eta_2 = \eta$. Note the monotonicity of each curve as a function of n and that $d_{2,\min}$, as well as $d_{1,\min}$, is always equal to zero.

though the numerical evidence strongly supports that these inequalities hold for an arbitrary active-detection efficiency mismatch. In Figs. 3 and 4, we report our numerical evidence for the specific mismatch model of Table I. Especially, one can see from these figures that the curve becomes monotonous as the efficiency mismatch increases.

In view of Eqs. (14) and (15), we find that the double-click probability d_{obs} and the effective-error probability e_{obs}

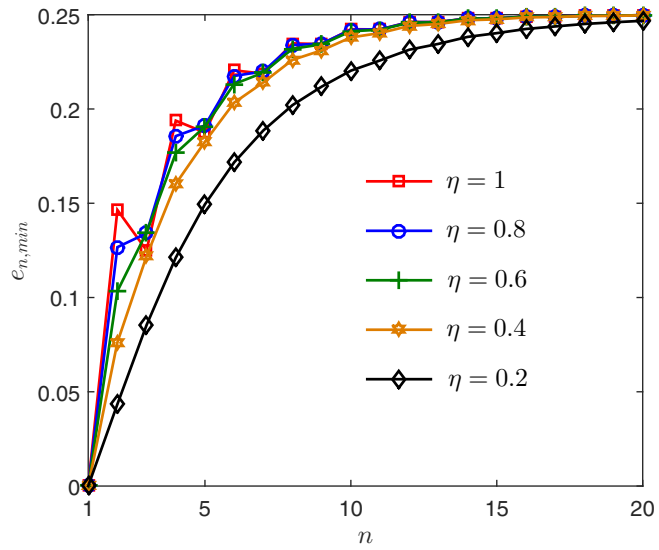

FIG. 4. The minimum effective-error probability $e_{n,\min}$ vs the photon number n received by Bob for the active-detection mismatch model of Table I with $\eta_1 = 1$ and $\eta_2 = \eta$. Note that $e_{3,\min}$ is a lower bound on $e_{n,\min}$ when $n \geqslant 3$ and that $e_{1,\min}$ is always equal to zero.

observed in practice satisfy

$$d_{\text{obs}} = \sum_{n=0}^{\infty} p_n \text{Tr}\left(\rho_{\text{AB}}^{(n)} F_{DC}^{(n)}\right) \geqslant (1 - p_0 - p_1 - p_2) d_{3,\min} \quad (17)$$

and

$$e_{\text{obs}} = \sum_{n=0}^{\infty} p_n \text{Tr}\left(\rho_{\text{AB}}^{(n)} F_{EE}^{(n)}\right) \geqslant (1 - p_0 - p_1 - p_2) e_{3,\min}, \quad (18)$$

by using that $\sum_{n=0}^{\infty} p_n = 1$. Hence, we can set the bound $b_2 \leqslant p_0 + p_1 + p_2$ as

$$b_2 = 1 - \min\left(\frac{d_{\text{obs}}}{d_{3,\min}}, \frac{e_{\text{obs}}}{e_{3,\min}}\right). \quad (19)$$

Note that for the observations simulated in Sec. IV, we found that $\frac{d_{\text{obs}}}{d_{3,\min}} < \frac{e_{\text{obs}}}{e_{3,\min}}$ and therefore the bound $b_2 = 1 - \frac{d_{\text{obs}}}{d_{3,\min}}$. Similarly, in view of Eq. (16), we have

$$e_{\text{obs}} = \sum_{n=0}^{\infty} p_n \text{Tr}\left(\rho_{\text{AB}}^{(n)} F_{EE}^{(n)}\right) \geqslant (1 - p_0 - p_1) e_{\min}. \quad (20)$$

Thus we can obtain a bound $b_1 \leqslant p_0 + p_1$ as

$$b_1 = 1 - \frac{e_{\text{obs}}}{e_{\min}}. \quad (21)$$

In this case, the double-click estimations do not lead to a nontrivial bound on b_1 as there exist two-photon states that do not lead to double clicks ($d_{2,\min} = 0$), see Fig. 3.

The above bounds b_1 and b_2 together with the flag-state squasher approach for the corresponding subspaces can be used in the key-rate optimization problem of Eq. (2) when the active-detection scheme is used.

2. *Passive-detection case*

The passive-detection scheme utilizes a 50/50 beam splitter to passively select a measurement basis, as shown in Fig. 1(b). Clearly, the probability that each output arm of the beam splitter contains at least one photon is given by $1 - 2^{-(n-1)}$. We therefore have the following expectations: (1) the probability of simultaneous photon detections at both output arms (referred to as cross clicks) would increase with the photon number n; and (2) in the limit of large n, the cross-click events would happen with near certainty. These motivate us to consider the associated cross-click operator

$$F_{CC} = \mathbb{1}^{\text{A}} \otimes M_{CC}^{\text{B}}, \quad (22)$$

with M_{CC}^{B} being Bob's cross-click POVM element (see Appendixes A and B of Ref. [14] for the derivation and expression of M_{CC}^{B}). To obtain bounds on the photon-number distribution using experimental observations, we thus consider the optimization problem

$$\begin{aligned} c_{n,\min} = \quad & \min_{\rho_{\text{AB}}^{(n)}} \text{Tr}\left(\rho_{\text{AB}}^{(n)} F_{CC}^{(n)}\right) \\ \text{subject to} \quad & \rho_{\text{AB}}^{(n)} \geqslant 0 \\ & \text{Tr}\left(\rho_{\text{AB}}^{(n)}\right) = 1 \,. \end{aligned} \quad (23)$$

Here, $F_{CC}^{(n)}$ is the n-photon component of the cross-click operator F_{CC}.

Again, we solve this optimization problem using the YALMIP toolbox [30] in MATLAB. The numerical solutions of

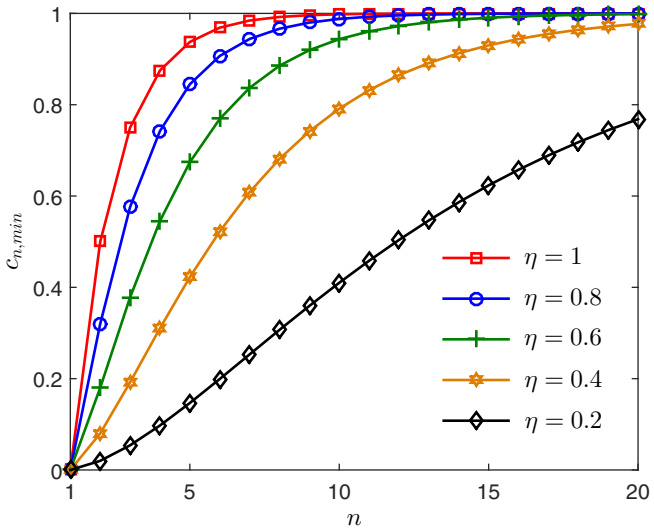

FIG. 5. The minimum cross-click probability $c_{n,\min}$ vs. the photon number n received by Bob for the passive-detection mismatch model of Table II with $\eta_1 = 1$ and $\eta_2 = \eta$. Note the monotonicity of each curve as a function of n, supporting the inequalities in Eqs. (24) and (25).

the optimization problem in Eq. (23) provide strong evidence that the cross-click probability $c_{n,\min}$ increases monotonically with n and converges to the unit value 1 for an arbitrary passive-detection efficiency mismatch. We would like to point out that any evaluation of secret-key rates using our approach requires solving an SDP problem, such as those in Eqs. (12), (13), and 23, thus allowing the validification of the working assumption for a chosen mismatch model and parameters. Particularly, the numerical evidence for our mismatch model and parameters is shown in Fig. 5, which suggests the following two inequalities

$$c_{n,\min} \geqslant c_{3,\min}, \forall n \geqslant 3, \tag{24}$$

and

$$c_{n,\min} \geqslant c_{2,\min}, \forall n \geqslant 2. \tag{25}$$

The inequality in Eq. (24) tells us that the cross-click probability c_{obs} observed in practice satisfies

$$c_{\text{obs}} = \sum_{n=0}^{\infty} p_n \text{Tr}\left(\rho_{\text{AB}}^{(n)} F_{CC}^{(n)}\right) \geqslant (1 - p_0 - p_1 - p_2) c_{3,\min}. \tag{26}$$

Here we used the fact that $\sum_{n=0}^{\infty} p_n = 1$. Thus we obtain a bound $b_2 \leqslant (p_0 + p_1 + p_2)$ as

$$b_2 = 1 - \frac{c_{\text{obs}}}{c_{3,\min}}. \tag{27}$$

Similarly, from Eq. (25) we can obtain a bound $b_1 \leqslant (p_0 + p_1)$ as

$$b_1 = 1 - \frac{c_{\text{obs}}}{c_{2,\min}}. \tag{28}$$

The above bounds b_1 and b_2 together with the flag-state squasher approach for the corresponding subspaces can be used in the key-rate optimization problem of Eq. (2) when the passive-detection scheme is used.

IV. SECRET-KEY RATES WITH SIMULATED OBSERVATIONS

As pointed out before, the method developed in Sec. III allows a security analysis of a QKD setup with an arbitrary detection-efficiency mismatch. Any such security analysis requires the determination of constraints on the probability of the state in a subspace containing at most a given number of photons, and then a reliable key-rate lower bound can be obtained using those constraints together with a flag-state squasher. We now illustrate our approach for the specific mismatch models of Tables I and II. As the security analysis usually requires as input some data observed in experiments, we replace here the experiments by simulations according to a simple quantum-optical model. We specify this toy model below, but it is important to point out that this toy model is not part of the security analysis, or in anyway an assumption on which our security proof itself is based. We also emphasize that the numerical values for the key rate reported in this section are reliable in the sense that they are computed according to the lower bound K_{lb} on the key rate [see Eq. (3)].

A. Data simulation

We study a BB84 protocol with an ideal single-photon source using polarization encoding. As described in Sec. II, at each round of the protocol Alice prepares one of four possible single-photon polarization states selected uniformly randomly. Bob can use either the active- or passive-detection scheme. In the active-detection scheme, we assume that at each round Bob can randomly select the key-generation basis with probability $p = 1/2$. The single photon prepared by Alice is transmitted through Eve's domain to Bob. We model the corresponding quantum channel as a depolarizing channel $\Lambda(\rho) = (1 - \omega)\rho + \omega \frac{1}{2}\mathbb{1}$ with depolarizing probability ω; additionally, the single-photon transmission efficiency over the channel is t. In order to introduce multiple detector clicks, Eve intercepts in our channel model with probability r the single photon and resends multiple photons to Bob. Specifically, Eve resends randomly polarized m photons in the state

$$\rho_m = \frac{1}{2m\pi} \int_0^{2\pi} d\theta (\hat{a}_\theta^\dagger)^m |0\rangle \langle 0| (\hat{a}_\theta)^m. \tag{29}$$

Here, the photon-creation operator $\hat{a}_\theta^\dagger$ is given in terms of the operators $\hat{a}_H^\dagger$ and $\hat{a}_V^\dagger$ of the respective linear polarizations as $\hat{a}_\theta^\dagger = \cos(\theta)\hat{a}_H^\dagger + \sin(\theta)\hat{a}_V^\dagger$. In our simulations, we will choose the photon number $m = 2$.

When applying the flag-state squasher approach, we choose to separate either the $(n \leqslant 1)$-photon or the $(n \leqslant 2)$-photon subspace from their respective complements. That is, we set the photon-number flag threshold to be $k = 1$ or 2. In our efficiency-mismatch models, we consider several spatial-temporal modes, in addition to the polarization mode. We note that the detectors used are assumed to be free of dark counts. In our toy quantum channel, we additionally assume that the optical signals are uniformly randomly distributed over all considered spatial-temporal modes.

B. Key rates in the absence of mismatch: trade-offs between transmission efficiency and detection efficiency

As mentioned in the introduction, when there is no efficiency mismatch between the detectors used in the measurement device, one can pull the detection inefficiency out of the detectors and into the channel action, creating an effective transmission loss. Consequently, the measurement device now is described by an ideal-detector setup for which a squashing model [23–25] exists, and so one can execute a full security proof. However, the resulting key rate might be conservatively low, because the existing security proof assumes that the photon loss during the actual transmission, as well as that due to the detection inefficiency, can be manipulated by Eve while under the original description of Bob's measurement device the photon loss inside of the device cannot be accessed by Eve. Such fact has been explicitly pointed out in literature such as in Ref. [31]. So while it is known that this is an overly pessimistic assumption, the issue is that proof techniques were missing to treat the security assuming the detection efficiency to be not accessible by Eve. We can tackle this question now with the techniques developed in this work.

With our numerical method, we can prove the security of a QKD protocol with arbitrary measurement operators as long as they are well characterized. In particular, we can characterize the detection efficiency of each detector in a measurement device, and so we can determine the corresponding measurement operators (see Appendixes A and B of Ref. [14]). In this way, we can study the individual effects of transmission efficiency and detection efficiency on the secret-key rate. To demonstrate these effects, for this particular result we assume for simplicity that each optical signal arriving at Bob contains no more than two photons, rather than using our flag-state squasher approach.

The results are shown in Fig. 6. From this figure, one can see that given the fixed total photon loss over both transmission and detection, Alice and Bob can distill more secret keys if they consider detection inefficiency and transmission loss separately rather than lumping these two kinds of loss together in the security proof. In particular, when the product $t\eta$ is fixed, the higher the value of t, the higher the secret-key rate is. On the other hand, when t and η are lumped together as an effective transmission efficiency $t\eta$, our numerical method provides the same key-rate lower bound as the standard security proofs with the help of the squashing model [23–25] for treating multiple-detection events. Specifically, the key-rate lower bound $\frac{1}{4}p_{\mathrm{det}}(1-2h(e))$, where p_{det} is the detection probability at the key-generation basis, e is the qubit error rate and $h(e)$ is the binary entropy function, is satisfied by the results plotted in Fig. 6 when $\eta = 1$.

We also performed numerical calculations, not presented here, which show that the higher the multi-photon probability r, the more significant improvement in the secret-key rate is achieved when separating t and η in the security proof. Particularly, we observed that when the optical signal has no multi-photon component (i.e., $r = 0$), the secret-key rate is independent of η as long as ω and $t\eta$ are fixed. However, in practice multiple-detection events occur due to the use of sources containing multi-photon states, cross talks in fibers, or dark counts in detectors.

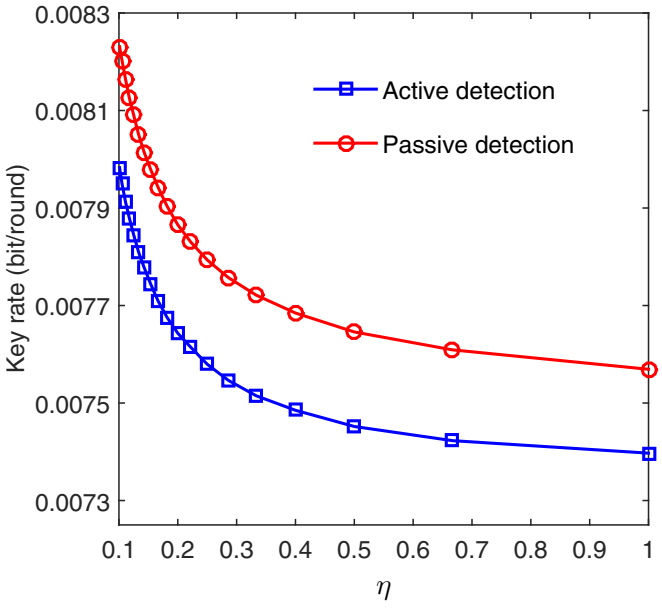

FIG. 6. Reliable key-rate lower bound in bits per round obtained by our numerical method vs the detection efficiency η of all detectors used in Bob's measurement device as shown in Fig. 1. We consider both the active- and passive-detection schemes. For data simulation, we fix the depolarizing probability $\omega = 0.05$, the multi-photon probability $r = 0.05$, and the product of transmission efficiency t and detection efficiency η to be $t\eta = 0.1$. We choose these values just for ease of graphical illustrations. We remark that under each detection scheme, the probability distribution observed by Alice and Bob does not change with η as long as the simulation parameters ω, r, and $t\eta$ are fixed.

C. Key rates with active-detection efficiency mismatch

Let us study the dependence of the secret-key rate on the detection-efficiency mismatch with the active-detection scheme. We consider two scenarios: In the *one-mode* scenario all photons received by Bob are in the same spatial-temporal mode, and the two detectors labeled by "H/D" and "V/A" in Fig. 1(a) have efficiencies η_1 and η_2, respectively; in the *two-mode* scenario the photons received by Bob can stay in one of two possible spatial-temporal modes or in a coherent superposition of the two spatial-temporal modes. The efficiency mismatch for the combinations of spatial-temporal modes and polarization detectors is shown as in Table I. For security proofs, we make use of and compare two different assumptions/techniques to deal with potential multi-photon signals arriving at Bob's detectors: we either assume that each signal received by Bob contains no more than two photons, or we prove security without such assumption. In the latter case, we apply a flag-state squasher with the photon-number flag threshold $k = 2$, and in the key-rate optimization problem of Eq. (2) we incorporate the lower bounds b_1 and b_2 on the photon-number probabilities $(p_0 + p_1)$ and $(p_0 + p_1 + p_2)$. These bounds are based on observations and are discussed in Sec. III C [see Eqs. (19) and (21)].

The typical results are shown in Fig. 7. We can make directly several observations from Fig. 7. (1) The larger the efficiency mismatch, the lower the secret-key rate is. There exists a threshold for the efficiency mismatch beyond which

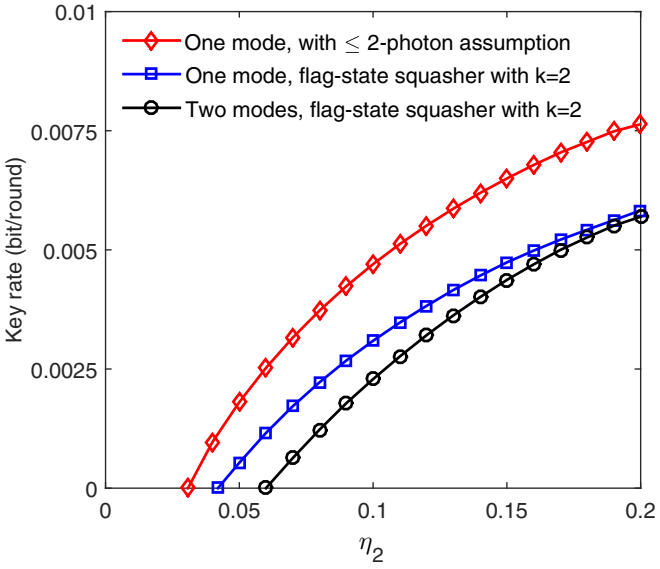

FIG. 7. Reliable key-rate lower bound in bits per round obtained by our numerical method vs. the detection efficiency η_2 of the detector labeled by "V/A" (for the signals stayed in the first spatial-temporal mode) in the active-detection scheme of Fig. 1(a). For data simulation, we fix the detection efficiency of the detector labeled by "H/D" (for the signals stayed in the first spatial-temporal mode) to $\eta_1 = 0.2$. We also fix the depolarizing probability $\omega = 0.05$, the multi-photon probability $r = 0.05$, and the transmission efficiency $t = 0.5$ (corresponding to 3dB loss). We remark that for the active-detection scheme the key rate scales linearly with the probability p for Bob to select the key-generation basis when other simulation parameters are fixed, and that for the results shown in this figure and the following Fig. 8 the probability p is fixed to be $1/2$ according to the data-simulation model detailed in Sec. IV A.

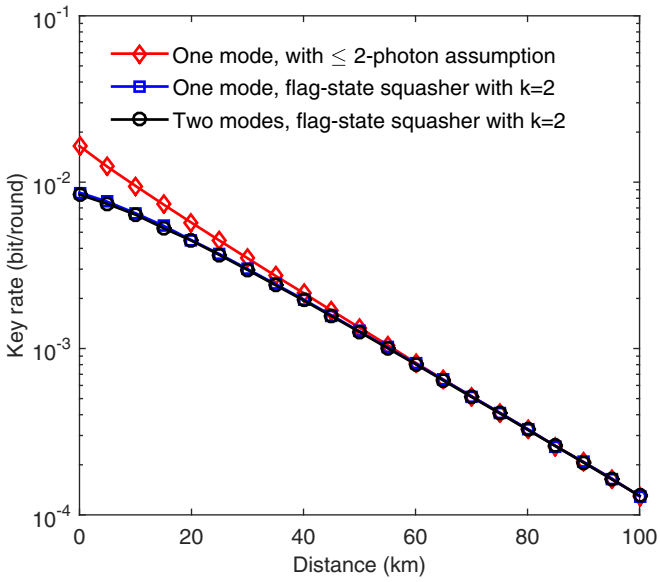

FIG. 8. Reliable key-rate lower bound in bits per round obtained by our numerical method vs the transmission distance in kilometers from Alice to Bob with the active-detection scheme of Fig. 1(a). For data simulation, we fix the detection efficiencies of the two detectors labeled by "H/D" and by "V/A" (for the signals stayed in the first spatial-temporal mode) to $\eta_1 = 0.2$ and $\eta_2 = 0.18$, respectively. We also fix the depolarizing probability $\omega = 0.05$ and the multiphoton probability $r = 0.05$. Note that when the same photon-number flag threshold $k = 2$ is used, the key-rate lower bound obtained for the case of mode-dependent efficiency mismatch is slightly lower than that for the case of mode-independent efficiency mismatch, although due to the use of a logarithmic scale in the plot such a difference is hard to be visible.

it is not possible for Alice and Bob to distill secret keys. (2) Making assumptions on Eve's attack strategy, such as assuming that no more than two photons are being resent from Eve to Bob, can overestimate the true secret-key rate computed according to the analysis without making that assumption. (3) The spatial-temporal-mode-dependent mismatch helps Eve to attack the QKD system. Our results show that Eve's corresponding freedom to manipulate the detection efficiencies decreases the secret-key rate. (4) If there is no efficiency mismatch, then the secret-key rate does not differ whether we consider one or two spatial-temporal modes. Note that in this case the lower bounds b_1 and b_2 in Eqs. (21) and (19) are independent of the number of spatial-temporal modes, and so is the key-rate optimization problem in Eq. (2).

We can also study the dependence of the secret-key rate on the transmission efficiency or distance when fixing other data-simulation parameters. For this, we assume that the transmission efficiency t is determined by the transmission distance L in kilometers according to $t = 10^{-L/50}$. Also, as mentioned in Sec. IV A we assume that the detectors used are free of dark counts. The typical results as shown in Fig. 8 suggest the following observations. First, with the increase of the transmission distance L, the key-rate lower bound obtained decreases. Particularly, when the distance L is large and in the absence of dark counts, the key-rate lower bound obtained decreases exponentially with the increase of L. Second, in the limit of large distance L, the key-rate lower bounds obtained under different efficiency-mismatch models or using different assumptions/techniques to handle multi-photon signals approach to each other.

D. Key rates with passive-detection efficiency mismatch

As in the active-detection scheme, we consider two scenarios: In the *single-mode* scenario all photons received by Bob are in the same spatial-temporal mode, and the four detectors labeled by "H," "V," "D," and "A" in Fig. 1(b) have efficiencies η_1, η_2, η_2, η_2 respectively; in the *four-mode* scenario the photons received by Bob can stay in one of four possible spatial-temporal modes or in a coherent superposition of the four spatial-temporal modes. The efficiency mismatch in the four spatial-temporal modes is shown as in Table II. In the security proofs, we again compare the flag-state squasher approach with the photon-number catoff assumption. Note that for the case with one spatial-temporal mode, we apply a flag-state squasher with the photon-number flag threshold $k = 2$, and at the same time we incorporate the lower bounds b_1 and b_2 in Eqs. (28) and (27). For the case with four spatial-temporal modes, instead we apply a flag-state squasher with the photon-number flag threshold $k = 1$, and exploit the corresponding photon-number distribution bound b_1. We do

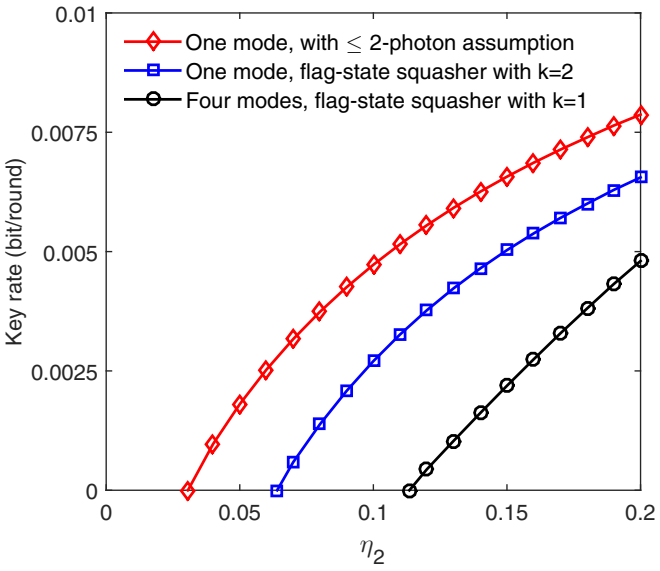

FIG. 9. Reliable key-rate lower bound in bits per round obtained by our numerical method vs. the detection efficiency η_2 of the detectors labeled by "V," "D," or "A" (for the signals stayed in the first spatial-temporal mode) in the passive-detection scheme of Fig. 1(b). For data simulation, we fix the detection efficiency of the detector labeled by "H" (for the signals stayed in the first spatial-temporal mode) to $\eta_1 = 0.2$. We also fix the depolarizing probability $\omega = 0.05$, the multiphoton probability $r = 0.05$, and the transmission efficiency $t = 0.5$ (corresponding to 3dB loss).

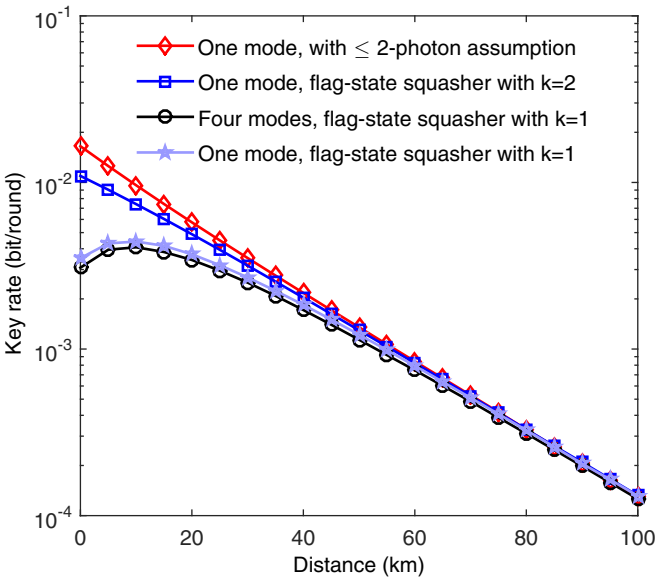

FIG. 10. Reliable key-rate lower bound in bits per round obtained by our numerical method vs the transmission distance in kilometers from Alice to Bob with the passive-detection scheme of Fig. 1(b). For data simulation, we fix the detection efficiencies $\eta_1 = 0.2$ and $\eta_2 = 0.18$, where η_1 and η_2 have the same meanings as those in Fig. 9. We also fix the depolarizing probability $\omega = 0.05$ and the multi-photon probability $r = 0.05$. Note that when the same photon-number flag threshold $k = 1$ is used, the key-rate lower bound obtained for the case of mode-dependent efficiency mismatch is slightly lower than that for the case of mode-independent efficiency mismatch. Also, by comparing the results obtained using the photon-number flag threshold $k = 1$ with those obtained using $k = 2$ in the case of one spatial-temporal mode, we can see that the usage of the photon-number flag threshold $k = 1$ can induce a nonmonotonic behavior of the obtained key-rate lower bound as a function of the transmission distance.

not use the tighter approach with the larger photon-number flag threshold $k = 2$, due to the large dimensionality of the corresponding key-rate optimization problem in the presence of four spatial-temporal modes. The dependence of the secret-key rate on the detection-efficiency mismatch is shown in Fig. 9. Similar to the active-detection case, the results in Fig. 9 suggest that the larger the efficiency mismatch, the lower the secret-key rate is. When the efficiency mismatch is large enough, it is not possible for Alice and Bob to distill secret keys. The results also suggest that spatial-temporal-mode-dependent mismatch helps Eve to attack the QKD system.

We remark that one cannot straightforwardly compare the robustness of the active- and passive-detection schemes against efficiency mismatch for distilling secret keys via Figs. 7 and 9. The reasons are as follows. First, there is no one-to-one correspondence between the two mismatch models given in Tables I and II, for the active- and passive-detection schemes respectively. Second, for spatial-temporal-mode-dependent mismatch, in the active-detection scheme, we considered two spatial-temporal modes and used the photon-number flag threshold $k = 2$ as well as the corresponding lower bounds on the photon-number probabilities $(p_0 + p_1)$ and $(p_0 + p_1 + p_2)$. However, in the passive-detection scheme we considered four spatial-temporal modes and used the smaller photon-number flag threshold $k = 1$ as well as the corresponding lower bound on the photon-number probability $(p_0 + p_1)$. The higher the photon-number flag threshold and the more constraints on the photon-number distribution, the higher the secret-key rate certified by our method is. We emphasize that here we have developed a general method for proving security of practical QKD protocols with efficiency mismatch. How to optimize our method and improve the secret-key rates certified will require future study.

We can also study the dependence of the secret-key rate on the transmission distance. Similar to the active-detection case, the typical results as shown in Fig. 10 suggest the following observations. First, in the limit of large transmission distance L, the key-rate lower bounds obtained under different efficiency-mismatch models or using different assumptions/techniques to handle multi-photon signals approach to each other. Second, when the transmission distance L is large, the key-rate lower bound obtained decreases exponentially with the increase of L. We note that when the distance L is small, the key-rate lower bound obtained by the flag-state squasher approach with the photon-number flag threshold $k = 1$ depends on L in a non-monotonic way. Such nonmonotonic behavior is understandable considering the following two competing facts: (1) with the increase of L, the cross-click probability decreases and so the lower bound on the photon-number probability $(p_0 + p_1)$ increases, which is helpful for our numerical method to distill secret keys; 2) with the increase of L, the detection probability decreases, which would result in a decrease of the key rate. By using the larger

photon-number flag threshold $k = 2$, the above nonmonotonic behavior disappears as we verified for the case with one spatial-temporal mode, see Fig. 10.

V. CONCLUSION

The security proof of QKD usually assumes that the threshold detectors used have the same detection efficiency. However, in practice, their detection efficiencies can show a mismatch, either due to the manufacturing and setup, or the influence by Eve (for example, by controlling the spatial-temporal-mode-dependent coupling of an optical signal with a detector). In this work we present an approach that allows to lower-bound the secret-key rate of a QKD setup with an arbitrary, but characterized detection-efficiency mismatch. We formulate the key-rate calculation as a convex-optimization problem. In order to prove security without relying on a catoff of photon numbers in the optical signal, we exploit the bounds on the photon-number distribution obtained directly from experimental observations with the help of semi-definite programs (SDPs), and simplify the key-rate optimization problem by introducing a flag-state squashing map. The key-rate optimization problem formulated is based on the practical measurement operators that depend on the characterized efficiency mismatch. Therefore we can study the effect of efficiency mismatch on the secret-key rate.

We illustrate the power of our method with numerical simulations, demonstrating that our method can be numerically well handled even in the presence of spatial-temporal-mode-dependent mismatch. Our method is especially applicable to free-space QKD where spatial-temporal-mode-dependent mismatch can be easily induced by Eve as demonstrated in Refs. [6–8].

Moreover, with our method, one can clearly see the individual effects of transmission loss and detection inefficiency on the secret-key rate (see Fig. 6). In the particular case of no mismatch, the simulation results show that our method provides a tighter lower bound on the secret-key rate than the squashing model [23–25] when we separate detection inefficiency (out of the domain of Eve) from transmission loss (in the domain of Eve).

Note added. After the submission of our work, we noticed that a related work by Trushechkin appeared on arXiv, see Ref. [32]. In contrast to our numerical bounds on the photon-number distribution obtained by solving semidefinite programs, Trushechkin [32] derived analytical bounds for the active-detection case. These analytical bounds can be combined with the flag-state squasher introduced in our work for a security proof without a catoff of photon numbers in the optical signal. Motivated by Trushechkin's work [32] and the construction of squashing models presented in Ref. [23], we can derive better analytical bounds on the photon-number distribution. We will present the details of these analytical bounds and their applications in the future work.

ACKNOWLEDGMENTS

We thank Shihan Sajeed, Poompong Chaiwongkhot, and Vadim Makarov for many useful discussions and comments. We gratefully acknowledge supports through the Office of Naval Research (ONR), the Ontario Research Fund (Ontario Research Fund), the Natural Sciences and Engineering Research Council of Canada (NSERC), and Industry Canada. Financial support for this work has been partially provided by Huawei Technologies Canada Co., Ltd.

APPENDIX: ALICE'S MEASUREMENT OPERATORS

In the source-replacement description of a BB84-QKD protocol with an ideal single-photon source using polarization encoding, the quantum system A held by Alice is two-dimensional and Alice performs ideal one-qubit measurements with perfect detection efficiency. In particular, Alice's measurement operators M_H^{A}, M_V^{A}, M_D^{A}, and M_A^{A} are ideal polarization-measurement operators in the one-photon space. In the basis $\{|1_H, 0_V\rangle_{\mathrm{A}}, |0_H, 1_V\rangle_{\mathrm{A}}\}$ of Alice's one-photon space over two polarization modes, these operators are represented as

$$M_H^{\mathrm{A}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad M_V^{\mathrm{A}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$
$$M_D^{\mathrm{A}} = 1/2 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad M_A^{\mathrm{A}} = 1/2 \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}. \tag{A1}$$

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[2] N. Lütkenhaus, Estimates for practical quantum cryptography, Phys. Rev. A **59**, 3301 (1999).

[3] Y. Zhao, C.-H. Fred Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78**, 042333 (2008).

[4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[5] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 349 (2011).

[6] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, Spatial mode side channels in free-space QKD implementations, IEEE J. Quantum Electron. **21**, 6600905 (2014).

[7] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch, Phys. Rev. A **91**, 062301 (2015).

[8] P. Chaiwongkhot, K. B. Kuntz, Y. Zhang, A. Huang, Jean-Philippe Bourgoin, S. Sajeed, N. Lütkenhaus, T. Jennewein,

and V. Makarov, Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence, Phys. Rev. A **99**, 062315 (2019).

[9] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[10] C.-H. Fred Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Security proof of quantum key distribution with detection efficiency mismatch, Quantum Inf. Comput. **9**, 131 (2009).

[11] L. Lydersen and J. Skaar, Security of quantum key distribution with bit and basis dependent detector flaws, Quantum Inf. Comput. **10**, 0060 (2010).

[12] M. K. Bochkov and A. S. Trushechkin, Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds, Phys. Rev. A **99**, 032308 (2019).

[13] J. Ma, Y. Zhou, X. Yuan, and X. Ma, Operational interpretation of coherence in quantum key distribution, Phys. Rev. A **99**, 062325 (2019).

[14] Y. Zhang and N. Lütkenhaus, Entanglement verification with detection-efficiency mismatch, Phys. Rev. A **95**, 042319 (2017).

[15] C. H. Bennett, G. Brassard, and N. David Mermin, Quantum Cryptography without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[16] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entanglement as a Precondition for Secure Quantum Key Distribution, Phys. Rev. Lett. **92**, 217903 (2004).

[17] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A **461**, 207 (2005).

[18] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Numerical approach for unstructured quantum key distribution, Nat. Commun. **7**, 11712 (2016).

[19] A. Winick, N. Lütkenhaust, and P. J. Coles, Reliable numerical key rates for quantum key distribution, Quantum **2**, 77 (2018).

[20] R. Renner, Security of Quantum Key Distribution, PhD. thesis, ETH, Zürich, Switzerland, 2005 (available as arXiv:quant-ph/0512258 version 2).

[21] M. Grant and S. Boyd, CVX: Matlab Software for Disciplined Convex Programming, version 2.1, 2014, http://cvxr.com/cvx.

[22] M. Grant and S. Boyd, Graph implementations for nonsmooth convex programs, *Recent Advances in Learning and Control* Lecture Notes in Control and Information Sciences (Springer-Verlag Limited, London, 2008), pp. 95–110.

[23] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Squashing Models for Optical Measurements in Quantum Communication, Phys. Rev. Lett. **101**, 093601 (2008).

[24] T. Tsurumaru and K. Tamaki, Security proof for quantum-key-distribution systems with threshold detectors, Phys. Rev. A **78**, 032302 (2008).

[25] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. Romero Alvarez, T. Moroder, and N. Lütkenhaus, Squashing model for detectors and applications to quantum-key-distribution protocols, Phys. Rev. A **89**, 012325 (2014).

[26] A. Ferenczi and N. Lütkenhaus, Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning, Phys. Rev. A **85**, 052310 (2012).

[27] M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto, Security of entanglement-based quantum key distribution with practical detectors, arXiv:0804.0891.

[28] A. Peres, Separability Criterion for Density Matrices, Phys. Rev. Lett. **77**, 1413 (1996).

[29] M. Horodecki, P. Horodecki, and R. Horodecki, Separability of mixed states: Necessary and sufficient conditions, Phys. Lett. A **223**, 1 (1996).

[30] J. Löfberg, YALMIP: A toolbox for modeling and optimization in matlab, in *Proceedings of the CACSD Conference* (IEEE, New York, 2004), pp. 284–289.

[31] M. Curty and N. Lütkenhaus, Effect of finite detector efficiencies on the security evaluation of quantum key distribution, Phys. Rev. A **69**, 042321 (2004).

[32] A. Trushechkin, Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case, arXiv:2004.07809.