Trusted Detector Noise Analysis for Discrete Modulation Schemes of Continuous-Variable Quantum Key Distribution

Jie Lin and Norbert Lütkenhaus

Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

Discrete-modulated continuous-variable quantum key distribution protocols are promising candidates for large-scale deployment due to the large technological overlap with deployed modern optical communication devices. The security of discrete modulation schemes has previously been analyzed in the ideal detector scenario in the asymptotic limit. In this work, we calculate asymptotic key rates against collective attacks in the trusted detector noise scenario. Our results show that we can thus cut out most of the effect of detector noise and obtain asymptotic key rates similar to those had we access to ideal detectors.

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] is a key establishment protocol with the provable information-theoretic security. Various QKD protocols with different advantages have been proposed, analyzed, and implemented. See, e.g., Refs. [3–6] for reviews. Continuous-variable (CV) QKD protocols [7–10] have competitive advantages in terms of massive deployment due to a significant overlap of devices used with those in the optical classical communications. Many experiments of CVQKD on both Gaussian modulation schemes such as Refs. [11–17] and discrete modulation schemes like Refs. [18–22] have been demonstrated.

On one hand, Gaussian modulation schemes are simpler to analyze theoretically than discrete modulation schemes, and they give secret key rates close to the theoretical limits [23,24]. On the other hand, continuous modulation itself is usually only approximated by a (relatively large) set of discrete modulation settings. This approximation needs to be taken into account during the full security analysis (see, e.g., Refs. [25–27]). Moreover, as Gaussian modulation schemes often require more resources in terms of randomness and classical postprocessing resources, discrete modulation schemes thus offer further simplification of implementation. However, in previous experimental demonstrations of discrete modulation schemes, either only effective entanglement has been verified [18,20],

which is a necessary precondition for QKD, or the security has been established only against a restricted subset of collective attacks [19,21]. By now, there are asymptotic security proofs against arbitrary collective attacks for binary [28], ternary [29] as well as quaternary modulation schemes and beyond [30,31]. Previous proofs for a general discrete modulation scheme [30,31] investigate the untrusted detector noise scenario where the imperfection of detectors can be controlled by Eve (and thus one can treat detectors as ideal). In reality, the amount of electronic noise of an off-the-shelf homodyne detector in a CVQKD experiment can be much higher than the channel excess noise. As a result, the key rate in the untrusted detector noise scenario drops very quickly to zero as the transmission distance increases. However, since detectors are securely located in Bob's laboratory where Eve is unable to access, it is reasonable to assume that Eve does not control detector imperfections especially those noise sources that are on the electronic circuitry, which is more remote from the quantum-mechanical part of the signal detection.

In this work, we extend our previous analysis [31] to the trusted detector noise scenario where detector imperfections (detector inefficiency and electronic noise) are not accessible to Eve. We remark that Gaussian modulation schemes have been analyzed in the trusted detector noise scenario [11,32–34] and it is known that the effects of electronic noise and detector inefficiency on the key rates are not very significant in the trusted detector noise scenario compared to the ideal detector scenario under realistic experimental conditions. As we show in this work, this observation also holds for discrete modulation schemes. However, we emphasize that our analysis is not a trivial application of the method used for Gaussian modulation protocols and instead we adopt a different approach. The

reason is that the previous method used in the Gaussian modulation protocols relies on the fact [35,36] that Eve's optimal attacks for Gaussian modulation schemes correspond to Gaussian channels, which make it easy to decouple the trusted detector noise from the channel noise when one looks at the covariance matrix. However, we cannot assume Gaussian channels here since Gaussian attacks are not expected to be optimal for discrete modulation schemes. In our analysis, based on a (commonly used) quantum optical model of the imperfect detector, we find its corresponding mathematical description in terms of positive operator-valued measure (POVM) and then use this POVM to construct observables corresponding to quantities that are measured experimentally. These observables are then used in our security proof. We also point out the crucial difference between our analysis and Ref. [37] for discrete modulation schemes: Our asymptotic analysis is valid against arbitrary collective attacks while Ref. [37] uses the Gaussian channel assumption and thus its security analysis [37] is restricted to Gaussian collective attacks.

Our main contributions of this work are finding a suitable POVM description of a noisy heterodyne detector and revising our previous analysis [31] by using a new set of constraints from this POVM in the numerical key-rate optimization problem [38,39]. Similar to our previous analysis, this method is applicable to both direct reconciliation and reverse reconciliation schemes. Moreover, we study the postselection of data [8] in the trusted detector noise scenario. As a concrete example, we apply our method to the quadrature phase-shift keying scheme with heterodyne detection and focus on the reverse reconciliation scheme. Our analysis here is still restricted to the asymptotic regime against collective attacks and we make the same photon-number cutoff assumption as in the previous works [30,31] to truncate the infinite-dimensional Hilbert space in order to perform the numerical calculation. From the numerical observation, we believe the results do not depend on the choice of cutoff when it is appropriately chosen. We direct the discussion about this assumption to Sec. III B of Ref. [31] and leave it for future work to provide an analytical justification of this assumption beyond the numerical evidences. To extend our analysis to the finite-key regime, we remark that we have recently extended the numerical method of Ref. [39] on which our analysis is based to include finite-key analysis [40]. However, there remain some technical challenges to solve before we can apply this method to this protocol and thus we leave the finite-key analysis for future work.

The rest of paper is outlined as follows. In Sec. II, we review the protocol and proof method in Ref. [31]. We then present a trusted detector noise model and the corresponding POVM description in Sec. III. In Sec. IV, we modify the key-rate optimization problem to take trusted detector noise into account. We discuss our simulation method in

Sec. V. We show the simulation results without postselection in Sec. VI and with postselection in Sec. VII. Finally, we summarize the results and provide insights for future directions in Sec. VIII. We present technical details in the Appendices.

II. BACKGROUND

Our key-rate calculation in the trusted detector noise scenario uses a similar proof method as in our previous work [31]; that is, we numerically perform the key-rate optimization problem [39] with a modified set of constraints. In particular, we discuss how to modify the key-rate optimization problem in Sec. IV based on the POVM description of a noisy heterodyne detector in Sec. III. To help understand this modification, we first review main ideas of the proof in Ref. [31].

For illustration, we focus on the quadrature phase-shift keying scheme with heterodyne detection. We remark that since the previous proof can be generalized to other discrete modulation schemes beyond four coherent states at the cost of more computational resources, our modified analysis for the trusted detector noise scenario can also be generalized in the same way. Moreover, one can apply a similar idea presented in this paper to study the homodyne detection scheme in the presence of trusted detector noise.

A. Quadrature phase-shift keying protocol

To begin with, we review the quadrature phase-shift keying (QPSK) scheme with heterodyne detection. The quantum part of the protocol consists of many repetitions of the following two steps: (1) Alice obtains a uniform random number $x \in \{0, 1, 2, 3\}$, selects the state $|\alpha_x\rangle = |\alpha e^{ix\pi/2}\rangle$ from the set $\{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}$ according to the value of x, and sends it to Bob. (2) Bob applies the heterodyne detection to the received state and obtains a measurement outcome $y \in \mathbb{C}$.

After the quantum-communication phase of the protocol, they proceed with the classical postprocessing part of the protocol including announcement, sifting, parameter estimation, key map (with discretization), error correction, and privacy amplification. In particular, the parameter estimation step is done according to the key-rate optimization problem in Eq. (22) discussed later. As the classical part is similar to other CVQKD protocols and is not the focus of our discussion, we highlight only the key-map step below for our discussion and skip the details of the remaining classical postprocessing procedures here. We direct readers to Ref. [31] for a more detailed description.

In the case of reverse reconciliation, for each measurement outcome y written as $y = |y|e^{i\theta}$, where $\theta \in [-\pi/4, 7\pi/4)$, Bob obtains a discretized value z according

to the following rule:

$$
z = \begin{cases} j, & \text{if } \theta \in \left[\dfrac{(2j-1)\pi}{4}, \dfrac{(2j+1)\pi}{4} \right) \text{ and } |y| \geq \Delta_a \\ \perp, & \text{otherwise,} \end{cases}
$$
(1)

where $j \in \{0, 1, 2, 3\}$ and Δ_a is a postselection parameter that needs to be optimized for the selected protocol and experimental parameters [41]. A protocol without postselection corresponds to setting $\Delta_a = 0$.

To perform the postselection of data in combination of reverse reconciliation, Bob announces positions where he obtains the value $\perp$. After removing the positions related to the value $\perp$, Alice's string $\vec{\mathbf{X}}$ consists of her random number x's in the remaining positions, and Bob's raw key string $\vec{\mathbf{Z}}$ consists of his discretized outcome z's left. (Alternatively, they may choose to announce and keep positions related to the value $\perp$ and let the privacy amplification subprotocol effectively remove those positions.) Alice and Bob may decide to recast their strings to binary strings before or during the error-correction step depending on their choice of the error-correction code. For the consistency of our presentation, we use the alphabet $\{0, 1, 2, 3\}$ and let $\mathbf{X}$ and $\mathbf{Z}$ denote the single-round version of $\vec{\mathbf{X}}$ and $\vec{\mathbf{Z}}$, respectively.

B. Review of security-proof method

1. Source-replacement scheme

The first step of our security proof is to apply the source-replacement scheme [42–45] to obtain an equivalent entanglement-based scheme for the given prepare-and-measure protocol. Then we proceed to prove the security of the entanglement-based scheme.

Given Alice's state ensemble $\{|\alpha_x\rangle, p_x\}$ (where $p_x = \frac{1}{4}$ for this protocol) for her preparation in the prepare-and-measure scheme, Alice effectively prepares a bipartite state $|\Psi\rangle_{AA'}$ in the source-replacement scheme, which is defined as

$$
|\Psi\rangle_{AA'} = \sum_{x=0}^{3} \sqrt{p_x} |x\rangle_A |\alpha_x\rangle_{A'},
$$
(2)

where $\{|x\rangle\}$ is an orthonormal basis for register A. Then Alice sends the register A' to Bob via an insecure quantum channel and keeps register A for her measurement described by the POVM $M^A = \{M_x^A = |x\rangle\langle x| : x \in \{0, 1, 2, 3\}\}$. The quantum channel that maps register A' to Bob's register B is described by a completely positive (CP) trace-preserving (TP) map, $\mathcal{E}_{A' \to B}$ and is assumed to be under Eve's control. Thus, Alice and Bob's joint state

ρ_{AB} before their measurements is

$$
\rho_{AB} = (\mathrm{id}_A \otimes \mathcal{E}_{A' \to B})(|\Psi\rangle\langle\Psi|_{AA'}),
$$
(3)

where id_A is the identity channel on Alice's system A.

When Alice performs a local measurement using her POVM $\{M_x^A\}$ on register A and obtains an outcome x, she effectively sends the coherent state $|\alpha_x\rangle$ to Bob. Bob's received state ρ_B^x conditioned on Alice's choice of x is

$$
\rho_B^x = \frac{1}{p_x} \mathrm{Tr}_A[\rho_{AB}(|x\rangle\langle x|_A \otimes \mathbb{1}_B)].
$$
(4)

Bob applies his POVM $M^B = \{M_y^B\}$ to register B to obtain his measurement outcomes. In the case of untrusted detector noise (or ideal heterodyne detector), the POVM of the heterodyne detection is $\{E_y = (1/\pi)|y\rangle\langle y| : y \in \mathbb{C}\}$, where $|y\rangle$ denotes a coherent state with complex amplitude y.

2. Key-rate optimization

The next step is to formulate the key-rate optimization problem for the entanglement-based scheme. One can rewrite the well-known Devetak-Winter formula [46] into the following form: [38,39]

$$
R^\infty = \min_{\rho_{AB} \in \mathbf{S}} D\big(\mathcal{G}(\rho_{AB}) \| \mathcal{Z}[\mathcal{G}(\rho_{AB})]\big) - p_{\mathrm{pass}} \delta_{\mathrm{EC}},
$$
(5)

where δ_{EC} is the actual amount of information leakage per signal pulse in the error-correction step, $D(\rho \| \sigma) = \mathrm{Tr}(\rho \log_2 \rho) - \mathrm{Tr}(\rho \log_2 \sigma)$ is the quantum relative entropy between two (subnormalized) density operators ρ and σ, $\mathcal{G}$ is a CP, trace nonincreasing map for postprocessing and $\mathcal{Z}$ is a pinching quantum channel for accessing results of the key map. The set $\mathbf{S}$ contains all density operators compatible with experimental observations. A more detailed discussion about the map $\mathcal{G}$ can be found in Appendix A of Ref. [31]. For the reverse reconciliation scheme, we can express the cost of error correction δ_{EC} by

$$
\delta_{\mathrm{EC}} = H(\mathbf{Z}) - \beta I(\mathbf{X}; \mathbf{Z}),
$$
(6)

where $H(\mathbf{Z})$ is the Shannon entropy of the raw key $\mathbf{Z}$, β is the reconciliation efficiency of the chosen error-correction code, and $I(\mathbf{X}; \mathbf{Z})$ is the classical mutual information between $\mathbf{X}$ and $\mathbf{Z}$.

Before we review the set of constraints as well as $\mathcal{G}$ and $\mathcal{Z}$ maps for the quadrature phase-shift keying scheme, we start with basic definitions. Given the annihilation operator $\hat{a}$ and creation operator $\hat{a}^\dagger$ of a single-mode state with the usual commutation relation $[\hat{a}, \hat{a}^\dagger] = \mathbb{1}$, we define the

quadrature operators $\hat{q}$ and $\hat{p}$, respectively, as

$$\hat{q} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a}), \quad \hat{p} = \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a}). \quad (7)$$

They obey the commutation relation $[\hat{q}, \hat{p}] = i\mathbb{1}$. To utilize the second-moment observations $\langle \hat{q}^2 \rangle$ and $\langle \hat{p}^2 \rangle$ to constrain ρ_{AB}, we previously defined the following two operators $\hat{n} = \frac{1}{2}(\hat{q}^2 + \hat{p}^2 - \mathbb{1}) = \hat{a}^\dagger \hat{a}$ and $\hat{d} = \hat{q}^2 - \hat{p}^2 = \hat{a}^2 + (\hat{a}^\dagger)^2$ [31]. The relation between these observables and the heterodyne detection POVM is highlighted in Sec. IV A.

For the untrusted detector noise (or ideal heterodyne detector) scenario, the key-rate optimization problem [31] is

$$\text{minimize} \quad D\big(\mathcal{G}(\rho_{AB}) \| \mathcal{Z}(\mathcal{G}(\rho_{AB}))\big)$$

subject to

$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{q})] = p_x \langle \hat{q} \rangle_x,$$
$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{p})] = p_x \langle \hat{p} \rangle_x,$$
$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{n})] = p_x \langle \hat{n} \rangle_x,$$
$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{d})] = p_x \langle \hat{d} \rangle_x, \quad (8)$$
$$\text{Tr}[\rho_{AB}] = 1,$$

$$\text{Tr}_B[\rho_{AB}] = \sum_{i,j=0}^{3} \sqrt{p_i p_j} \langle \alpha_j | \alpha_i \rangle |i\rangle \langle j|_A,$$

$$\rho_{AB} \geq 0,$$

where the index x runs over the set $\{0, 1, 2, 3\}$ and $\langle \hat{q} \rangle_x, \langle \hat{p} \rangle_x, \langle \hat{n} \rangle_x$, and $\langle \hat{d} \rangle_x$ denote the corresponding expectation values of operators $\hat{q}, \hat{p}, \hat{n}$, and $\hat{d}$ for the conditional state ρ_B^x, respectively.

As indicated in Fig. 1, the protocol can perform postselection of data. To perform postselection, we define the region operators in Ref. [31] as

$$R_j = \frac{1}{\pi} \int_{\Delta_a}^{\infty} \int_{(2j-1)\pi/4}^{(2j+1)\pi/4} r |re^{i\theta}\rangle \langle re^{i\theta}| \, d\theta \, dr \quad (9)$$

for $j \in \{0, 1, 2, 3\}$. The area of integration for each operator corresponds to a region shown in Fig. 1.

The postprocessing map $\mathcal{G}$ in the reverse reconciliation scheme is given by $\mathcal{G}(\sigma) = K\sigma K^\dagger$ for any input state σ, where the Kraus operator K is

$$K = \sum_{z=0}^{3} |z\rangle_R \otimes \mathbb{1}_A \otimes (\sqrt{R_z})_B, \quad (10)$$

where $\{|0\rangle_R, |1\rangle_R, |2\rangle_R, |3\rangle_R\}$ is the standard basis for register R. The pinching quantum channel $\mathcal{Z}$ is given by
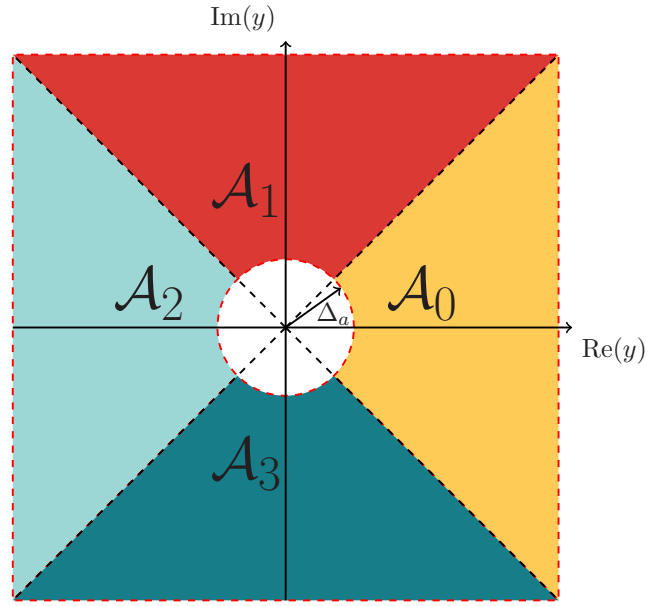

FIG. 1. Key map for quadrature phase-shift keying scheme in terms of Bob's measurement outcome $y \in \mathbb{C}$. Each colored region $\mathcal{A}_j$ corresponds to a discretized key value j. The measurement outcome in the central disk with a radius Δ_a is discarded during the postselection of data and is mapped to the symbol $\perp$.

projections $\{|j\rangle\langle j|_R \otimes \mathbb{1}_{AB} : j \in \{0, 1, 2, 3\}\}$ as

$$\mathcal{Z}(\sigma) = \sum_{j=0}^{3} (|j\rangle\langle j|_R \otimes \mathbb{1}_{AB}) \sigma (|j\rangle\langle j|_R \otimes \mathbb{1}_{AB}). \quad (11)$$

III. NOISY HETERODYNE DETECTION

In this section, we present one physical model for a noisy heterodyne detector and give the corresponding POVM description. We start with a slightly more general model and then we make a simplification for the ease of calculation at the end of this section. This simplified model then reduces to a model commonly used in the literature.

A. Trusted detector noise model

As a heterodyne detector consists of two homodyne detectors and a beam splitter, we consider imperfections in each homodyne detector. A homodyne detector may have nonunity detector efficiency and also have some amount of electronic noise, which is the additional noise introduced to the measured data by its electronic components. In an experiment, one is able to measure the amount of electronic noise and the value of detector efficiency by a calibration routine. To model a realistic homodyne detector with nonunity detector efficiency and some amount of electronic noise, we use a quantum optical model, which is used in Refs. [11,32–34,37], although the source of this electronic noise is in the actual electronics part of the

detector. An alternative view of the electronic noise is that we can think about the detector as being a perfect detector followed by some classical postprocessing of the data, which adds noise. One should note that in a trusted device scenario, the characterization of the actual noise should be experimentally verified. Our physical model is chosen for convenience of calculating the POVM of the actual measurement. We depict this physical model of a noisy heterodyne detector in Fig. 2. In this diagram, we consider a more general case where two homodyne detectors have different imperfections. We label the efficiency of the homodyne detector used for q quadrature measurement as η_1 and its electronic noise as ν_1 (expressed in shot-noise units). Similarly, the efficiency of the homodyne detector used for p quadrature measurement is labeled as η_2 and its electronic noise is labeled as ν_2.

Since our treatment for each homodyne detector in this heterodyne setup is the same, we take one homodyne detector (shown in each dashed box in Fig. 2) as an example and treat the other one similarly by using its corresponding efficiency and electronic noise. An imperfect homodyne detector with its efficiency $\eta_j < 1$ and electronic noise $\nu_j \geq 0$ (for $j = 1$ or 2) can be modeled by a beam splitter placed before a perfect homodyne detector with the following specification. (1) The ratio of transmission to reflection of this beam splitter is $\eta_j : 1 - \eta_j$. (2) One input port of this beam splitter is the signal pulse and the other input port is a thermal state used to model
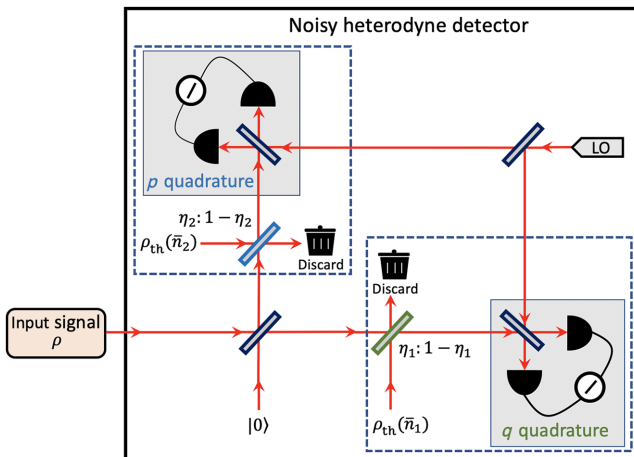

FIG. 2. Physical model for a noisy heterodyne detector. The homodyne detector for the q quadrature measurement has detector efficiency η_1 and electronic noise ν_1. The homodyne detector for the p quadrature measurement has detector efficiency η_2 and electronic noise ν_2. The notation $\rho_{\text{th}}(\bar{n})$ stands for a thermal state with a mean photon number $\bar{n}$. In particular, $\bar{n}_1 = \nu_1/[2(1 - \eta_1)]$ and $\bar{n}_2 = \nu_2/[2(1 - \eta_2)]$ (see main text for more explanations). Beam splitters are 50:50 unless specified otherwise. Each homodyne detector inside a gray box is ideal. Each dashed box encloses the physical model for a noisy homodyne detector. LO stands for local oscillator.

electronic noise, which is equivalent to sending one mode of a two-mode squeezed vacuum state (EPR state) to the beam splitter. Each quadrature's variance of this ancillary thermal state is related to the value of electronic noise ν_j. More specifically, it is $[1 + \nu_j/(1 - \eta_j)]N_0$ [11], where $N_0 = 1/2$ denotes the shot-noise variance. In Fig. 2, we choose to parametrize the thermal state in terms of its mean photon number as $\bar{n}_j = \nu_j/[2(1 - \eta_j)]$ instead of the variance of each quadrature, which is convenient for writing of expressions in later sections [47]. We note that this way of modeling electronic noise is valid when $\eta_j \neq 1$. Furthermore, we assume $\eta_j \neq 0$. That is, we consider the case $\eta_j \in (0, 1)$, which is the case of a realistic detector of our interest.

In the next section, we derive the POVM corresponding to this detector model. We then choose to consider a simplified scenario where these two homodyne detectors are identical for the purpose of illustration and the ease of numerical calculation. That is, we later assume they both have the same detector efficiency $\eta_1 = \eta_2 =: \eta_d$ and the same electronic noise $\nu_1 = \nu_2 =: \nu_{\text{el}}$.

B. POVM description

We use the Wigner function formulation to find the POVM $\{G_y : y \in \mathbb{C}\}$ corresponding to this noisy heterodyne detector model. When two homodyne detectors give two real numbers q_s and p_s for q and p quadrature measurements, we label the outcome as $y = q_s + ip_s$. By considering $\text{Tr}(\rho G_y)$ for an arbitrary input density operator ρ to the noisy heterodyne detector, we are able to find the Wigner function W_{G_y} of the POVM element G_y as

$$
\begin{aligned}
W_{G_y}(\gamma) = {} & \frac{1}{\sqrt{\eta_1 \eta_2}\pi} \frac{2}{\pi} \frac{1}{\sqrt{1 + \frac{2(1-\eta_1+\nu_1)}{\eta_1}}} \frac{1}{\sqrt{1 + \frac{2(1-\eta_2+\nu_2)}{\eta_2}}} \\
& \times \exp\left\{ \frac{-2[\text{Re}(\gamma) - \frac{1}{\sqrt{\eta_1}}\text{Re}(y)]^2}{1 + \frac{2(1-\eta_1+\nu_1)}{\eta_1}} \right\} \\
& \times \exp\left\{ \frac{-2[\text{Im}(\gamma) - \frac{1}{\sqrt{\eta_2}}\text{Im}(y)]^2}{1 + \frac{2(1-\eta_2+\nu_2)}{\eta_2}} \right\}. \quad (12)
\end{aligned}
$$

By comparing this Wigner function with that of a displaced squeezed thermal state, we can identify that the POVM element G_y is a projection onto a displaced squeezed thermal state up to a prefactor $1/(\sqrt{(\eta_1\eta_2)}\pi)$. We give a full derivation of this Wigner function and the explicit parameters for displacement, squeezing, and thermal state mean photon number in terms of detector parameters η_1, η_2, ν_1, and ν_2 in Appendix A.

For the rest of the paper, we restrict our discussion to a simpler scenario where we assume both homodyne detectors have the same imperfection for the ease of numerical

calculation and for the purpose of illustration. We discuss how to perform the calculation in the general case in Appendix B. In this simple case, we set $\eta_1 = \eta_2 = \eta_d$ and $\nu_1 = \nu_2 = \nu_{\mathrm{el}}$ in Eq. (12). This equation is simplified to be

$$W_{G_y}(\gamma) = \frac{1}{\eta_d \pi} \frac{2}{\pi} \frac{1}{1 + \frac{2(1-\eta_d+\nu_{\mathrm{el}})}{\eta_d}} \exp\left[\frac{-2|\gamma - \frac{y}{\sqrt{\eta_d}}|^2}{1 + \frac{2(1-\eta_d+\nu_{\mathrm{el}})}{\eta_d}} \right].$$
(13)

One can observe that it is the Wigner function of a displaced thermal state apart from the prefactor $1/(\eta_d \pi)$. Therefore, the POVM element G_y in this case is a scaled projection onto a displaced thermal state. More precisely,

$$G_y = \frac{1}{\eta_d \pi} \hat{D}\left(\frac{y}{\sqrt{\eta_d}} \right) \rho_{\mathrm{th}}\left(\frac{1-\eta_d+\nu_{\mathrm{el}}}{\eta_d} \right) \hat{D}^\dagger\left(\frac{y}{\sqrt{\eta_d}} \right),$$
(14)

where $\hat{D}(y/\sqrt{\eta_d})$ is the displacement operator with the amount of displacement $y/\sqrt{\eta_d}$ and $\rho_{\mathrm{th}}[(1 - \eta_d + \nu_{\mathrm{el}})/\eta_d]$ is a thermal state with the mean photon number $(1 - \eta_d + \nu_{\mathrm{el}})/\eta_d$, which can be expressed in the photon-number basis as

$$\rho_{\mathrm{th}}(\bar{n}) = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(1 + \bar{n})^{n+1}} |n\rangle\langle n|.$$
(15)

Later in Sec. IV, we need to express operators defined in terms of POVM elements G_y's in the photon-number basis for the numerical key-rate calculation. Analytical expressions of matrix elements $\langle m | G_y | n \rangle$ are known in the literature [48] and shown in Appendix B.

Let us end this section with a few remarks about the simplification considered here. Firstly, as we later define operators involving integrals of POVM elements G_y's and need to find their matrix representations in the photon-number basis for the numerical key-rate calculation, we are able to find efficiently computable analytical expressions for these operators under this simplification. Without this simplification, one may need to perform some numerical integrations. We emphasize that the principles presented in this work also hold for the general case and we choose to present results based on this simplified case for the ease of calculation. Secondly, with this simplification, our detector model is then optically equivalent to the detector model used in other works [32,34]. Thirdly, if two homodyne detectors in the heterodyne detection scheme do not have the same imperfection, one can instead use the POVM in the general case by following the procedure outlined in Appendix B 2 despite being more numerically challenging.

IV. KEY-RATE OPTIMIZATION PROBLEM

We start with a reformulation of the optimization problem in Eq. (8) in the untrusted detector noise scenario,

which serves as a basis for our modification in the trusted detector noise scenario. The purpose of this reformulation is that once we substitute the POVM of the noisy heterodyne detector in place of the one for the ideal heterodyne detector, we can easily formulate the optimization problem in the trusted detector noise scenario. Specifically, we change Bob's POVM $\{M_y^B\}$ from the ideal heterodyne detection $\{E_y = \frac{1}{\pi}|y\rangle\langle y|\}$ to the POVM description of the noisy heterodyne detection $\{G_y\}$ found in Eq. (14). Moreover, compared with our previous work [31], some constraints are modified to match with how data are processed in a typical experiment.

A. Reformulation of the optimization problem in the untrusted detector noise scenario

We reconsider the key-rate optimization problem in the untrusted detector noise scenario by rewriting region operators in Eq. (9) and observables in Eq. (8) in terms of the POVM of an ideal heterodyne detector $\{E_y\}$. In the case of ideal heterodyne detection, the POVM description of Bob's measurement $\{M_y^B\}$ is $M_y^B = E_y = (1/\pi)|y\rangle\langle y|$, the projection onto a coherent state $|y\rangle$. By writing $y = re^{i\theta}$ in the polar coordinate and integrating over the corresponding region $\mathcal{A}_j$, we obtain Eq. (9). If we rewrite Eq. (9) in terms of M_y^B, we see region operators R_j's are defined by

$$R_j = \int_{y \in \mathcal{A}_j} M_y^B d^2y,$$
(16)

where the region of integration $\mathcal{A}_j$ in the complex plane is shown in Fig. 1 and $d^2y = d\mathrm{Re}(y)d\mathrm{Im}(y)$.

From the heterodyne detection, we obtain a probability density function $P(y)$ for the outcome $y \in \mathbb{C}$. [We obtain such a probability density function for each conditional state ρ_B^x. While it is more proper to denote this conditional probability density function as $P(y|x)$, for simplicity of notation in this section, we use $P(y)$.] When the heterodyne detector is ideal, this probability density function is the Husimi Q function. In particular, as discussed in our previous work [31], the expectation values of operators $\hat{q}, \hat{p}, \hat{n}$, and $\hat{d}$ defined in Sec. II B are related to the Q function via

$$\langle \hat{q} \rangle_x = \frac{1}{\sqrt{2}} \int (y + y^*) Q_x(y) d^2y,$$

$$\langle \hat{p} \rangle_x = \frac{i}{\sqrt{2}} \int (y^* - y) Q_x(y) d^2y,$$
(17)

$$\langle \hat{n} \rangle_x = \int (|y|^2 - 1) Q_x(y) d^2y,$$

$$\langle \hat{d} \rangle_x = \int [y^2 + (y^*)^2] Q_x(y) d^2y,$$

where the subscript x labels the conditional state ρ_B^x.

In general, one may be interested in a quantity like $\int f(y,y^*)P(y)d^2y$ where $f(y,y^*)$ is a real-valued function on y and y^* such that the integral converges. Such a quantity can be described as the expectation value of an observable that is defined in the following way:

$$\hat{O} = \int f(y,y^*)M_y^B d^2y \qquad (18)$$

since

$$\text{Tr}[\rho\,\hat{O}] = \int d^2y\, f(y,y^*)\text{Tr}(\rho M_y^B)$$
$$= \int d^2y\, f(y,y^*)P(y). \qquad (19)$$

In other words, operators constructed in this way correspond to expectation values $\int f(y,y^*)P(y)d^2y$ obtained in an experiment. By comparing Eq. (19) to Eq. (17) and identifying $P(y)$ by $Q_x(y)$, we observe the following choices of $f(y,y^*)$ for $\hat{q}$, $\hat{p}$, $\hat{n}$, and $\hat{d}$:

$$\hat{q} \longleftrightarrow f(y,y^*) = \frac{y+y^*}{\sqrt{2}},$$
$$\hat{p} \longleftrightarrow f(y,y^*) = \frac{i(y^*-y)}{\sqrt{2}},$$
$$\hat{n} \longleftrightarrow f(y,y^*) = |y|^2 - 1, \qquad (20)$$
$$\hat{d} \longleftrightarrow f(y,y^*) = y^2 + (y^*)^2.$$

We remark that this way of defining these observables corresponds to the antinormally ordered expansion of operators [49,50].

B. Revised optimization problem in the trusted detector noise scenario

In Ref. [31], we chose observables $\{\hat{O}\} = \{\hat{q},\hat{p},\hat{n},\hat{d}\}$ by using $M_y^B = E_y$ in Eq. (18) for the untrusted detector noise scenario. In this work, we change to a new set of observables $\{\hat{q},\hat{p},\hat{n}+\hat{d}/2+\mathbb{1},\hat{n}-\hat{d}/2+\mathbb{1}\}$, which gives the same key rates as the old one since the last two observables in this new set are linear combinations of observables $\hat{n}$ and $\hat{d}$ as well as the identity operator. This new set of observables corresponds to the set of $\{f(y,y^*)\} = \{\sqrt{2}\text{Re}(y), \sqrt{2}\text{Im}(y), 2\text{Re}(y)^2, 2\text{Im}(y)^2\}$ [51]. The sole purpose of this change compared with Ref. [31] is to make the data postprocessing in an agreement with the typical classical postprocessing in an experiment. That is, in an experiment, when a heterodyne detection gives two real numbers q_s and p_s which we set $\text{Re}(y) = q_s$ and $\text{Im}(y) = p_s$, one usually computes variances of $\text{Re}(y)$ and $\text{Im}(y)$ by computing the expectation values of $\text{Re}(y)^2$ and $\text{Im}(y)^2$ in addition to expectation values of $\text{Re}(y)$ and $\text{Im}(y)$.

In the trusted detector noise scenario, we need to substitute M_y^B in Eqs. (16) and (18) by G_y. To distinguish operators defined in this way from the first and second moment of quadrature operators $\hat{q}$ and $\hat{p}$, we call first-moment observables $\hat{F}_Q$ and $\hat{F}_P$ and second-moment observables $\hat{S}_Q$ and $\hat{S}_P$. More explicitly, they are defined as

$$\hat{F}_Q = \int \frac{y+y^*}{\sqrt{2}} G_y d^2y,$$
$$\hat{F}_P = \int \frac{i(y^*-y)}{\sqrt{2}} G_y d^2y,$$
$$\hat{S}_Q = \int \left(\frac{y+y^*}{\sqrt{2}}\right)^2 G_y d^2y, \qquad (21)$$
$$\hat{S}_P = \int \left[\frac{i(y^*-y)}{\sqrt{2}}\right]^2 G_y d^2y.$$

Then the revised key-rate optimization problem becomes

minimize $\quad D(\mathcal{G}(\rho_{AB})\|\mathcal{Z}[\mathcal{G}(\rho_{AB})])$

subject to

$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{F}_Q)] = p_x\langle\hat{F}_Q\rangle_x,$$
$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{F}_P)] = p_x\langle\hat{F}_P\rangle_x,$$
$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{S}_Q)] = p_x\langle\hat{S}_Q\rangle_x,$$
$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{S}_P)] = p_x\langle\hat{S}_P\rangle_x, \qquad (22)$$
$$\text{Tr}[\rho_{AB}] = 1,$$
$$\text{Tr}_B[\rho_{AB}] = \sum_{i,j=0}^{3} \sqrt{p_i p_j}\langle\alpha_j|\alpha_i\rangle|i\rangle\langle j|_A,$$
$$\rho_{AB} \geq 0,$$

where the index x runs over the set $\{0, 1, 2, 3\}$ and the Kraus operator for the postprocessing map $\mathcal{G}$ has the same form as in Eq. (10) but now with the region operators defined in terms of G_y's in Eq. (16).

In Appendix B, we discuss how to represent these operators in the photon-number basis. Combining with the photon-number cutoff assumption [i.e., $\rho_{AB} = (\mathbb{1}_A \otimes \Pi_N)\rho_{AB}(\mathbb{1}_A \otimes \Pi_N)$, where N is the cutoff photon number and Π_N is the projection onto the subspace spanned by the photon-number states from 0 to N photons], we can directly solve this key-rate optimization problem in Eq. (22) numerically. We direct readers to Sec. IV B of Ref. [31] for the discussion about the numerical algorithm for the optimization problem and its performance.

V. SIMULATION METHOD

In an experiment, the expectation values shown in the optimization problem in Eq. (22) can be obtained from

some suitable postprocessing of noisy heterodyne detection results. Without doing experiments, we perform simulations of a corresponding experiment with a noisy heterodyne detector to obtain those expectation values. With these values specified, one can solve the key-rate optimization problem using a numerical convex optimization package to obtain numerical results. We emphasize that our security-proof technique does not depend on the specific channel model used for the simulation.

A. Channel model for simulation

To understand how the protocol behaves in the trusted detector noise scenario, we simulate the quantum channel by using a realistic physical channel in an honest implementation of the protocol. A realistic physical channel in the context of the optical fiber communication can be modeled by a phase-invariant Gaussian channel with the transmittance η_t and excess noise ξ. In a typical fiber for optical communication, the attenuation coefficient is 0.2 dB/km and thus $\eta_t = 10^{-0.02L}$ for a distance L in kilometers. The excess noise ξ is defined as

$$\xi = \frac{(\Delta q_{\text{obs}})^2}{(\Delta q_{\text{vac}})^2} - 1, \quad (23)$$

where $(\Delta q_{\text{vac}})^2 = N_0 = 1/2$ is the variance in q quadrature of the vacuum state and $(\Delta q_{\text{obs}})^2$ is the observed variance in q quadrature of the measured signal state. As the value of ξ is normalized with respect to the vacuum variance, the channel excess noise ξ is reported in the shot-noise units (SNU) and independent of different conventions of defining quadrature operators.

Apart from the shot noise, there are several contributions to the total noise in the measurement data such as preparation noise, detector noise, and noises introduced in the fiber due to Raman scattering. As we treat the detection noise as trusted, we assume all other contributions are under Eve's control. In other words, all additional noises beyond the shot noise except for the detector noise become a part of the effective quantum channel regardless of the physical origin of each noise component, and they contribute to the value of the excess noise ξ. In the literature, the value of the excess noise ξ is commonly reported at the input of the quantum channel, which corresponds to measuring $(\Delta q_{\text{obs}})^2$ at the output of Alice's lab. By choosing this convention of reporting the value of excess noise, we may alternatively imagine that this effective quantum channel first introduces the amount of excess noise ξ to the signal state at the input of the channel and the rest of this quantum channel is then lossy but noise-free. Under this channel model, a coherent state $|\alpha\rangle$, after transmitting through this quantum channel, becomes a displaced thermal state centered at $\sqrt{\eta_t}\alpha$ with its variance $\frac{1}{2}(1 + \eta_t\xi)$ for each quadrature.

B. Simulated statistics

From our simulation, the simulated state σ_B^x conditioned on the choice of x is a displaced thermal state whose Wigner function is

$$W_{\sigma_B^x}(\gamma) = \frac{1}{\pi}\frac{1}{\frac{1}{2}(1 + \eta_t\xi)}\exp\left[-\frac{|\gamma - \sqrt{\eta_t}\alpha_x|^2}{\frac{1}{2}(1 + \eta_t\xi)}\right]. \quad (24)$$

When Bob applies his heterodyne measurement described by the POVM $\{G_y\}$, the probability density function $P(y|x)$ for the measurement outcome y conditioned on Alice's choice x is

$$P(y|x) = \frac{1}{\pi\left(1 + \frac{1}{2}\eta_d\eta_t\xi + v_{\text{el}}\right)}\exp\left[-\frac{|y - \sqrt{\eta_d\eta_t}\alpha_x|^2}{1 + \frac{1}{2}\eta_d\eta_t\xi + v_{\text{el}}}\right]. \quad (25)$$

The observables defined in Eq. (21) have the following expectation values from the simulation:

$$\begin{aligned}
\langle\hat{F}_Q\rangle_x &= \sqrt{2\eta_d\eta_t}\text{Re}(\alpha_x), \\
\langle\hat{F}_P\rangle_x &= \sqrt{2\eta_d\eta_t}\text{Im}(\alpha_x), \\
\langle\hat{S}_Q\rangle_x &= 2\eta_d\eta_t\text{Re}(\alpha_x)^2 + 1 + \frac{1}{2}\eta_d\eta_t\xi + v_{\text{el}}, \\
\langle\hat{S}_P\rangle_x &= 2\eta_d\eta_t\text{Im}(\alpha_x)^2 + 1 + \frac{1}{2}\eta_d\eta_t\xi + v_{\text{el}}.
\end{aligned} \quad (26)$$

C. Estimation of error-correction cost

We estimate the cost of error correction from the simulated statistics. From the probability density function $P(y|x)$ shown in Eq. (25), we can obtain the joint probability distribution $\widetilde{P}(x,z)$ for Alice's choice $\mathbf{X} = x$ and Bob's discretized key value $\mathbf{Z} = z$ by the following integral:

$$\widetilde{P}(z|x) = \int_{\Delta_a}^{\infty} dr\, r \int_{[(2z-1)/4]\pi}^{[(2z+1)/4]\pi} d\theta P(re^{i\theta}|x). \quad (27)$$

Since $\widetilde{P}(x) = p_x = \frac{1}{4}$, we then obtain the joint probability distribution $\widetilde{P}(x,z) = \widetilde{P}(z|x)\widetilde{P}(x)$. Using the definition of $I(\mathbf{X};\mathbf{Z})$ in terms of $\widetilde{P}(x,z)$, we can approximate the cost of error correction by Eq. (6) for the reverse reconciliation scheme considered in this work. When Δ_a is not zero, that is, in the presence of postselection, the sifting factor p_{pass} is the sum of $\widetilde{P}(x,z)$ over $x, z \in \{0, 1, 2, 3\}$. We then renormalize the probability distribution before plugging it in the definition of $I(\mathbf{X};\mathbf{Z})$.

For the purpose of illustration, we choose the error-correction efficiency β to be 95% for our simulations, which is around typical values for the state-of-the-art error-correction codes (see, e.g., Ref. [52]).

VI. KEY RATE IN THE ABSENCE OF POSTSELECTION

In this section, we present results when no postselection is performed, that is, $\Delta_a = 0$. We make two comparisons. The first one is to compare key rates in the trusted and untrusted detector noise scenarios. The second one is to analyze how different imperfections in detectors affect key rates in the trusted detector noise scenario.

A. Comparison between trusted and untrusted detector noise scenarios

For this comparison, we supply the same set of simulated data from Eq. (26) to the optimization problem for the untrusted detector noise scenario in Eq. (8) and the one for the trusted detector noise scenario in Eq. (22). For simulation, we choose parameters $\eta_d = 0.719$, $\nu_{el} = 0.01$ from Ref. [14] for illustration. The result is shown in Fig. 3.

As we can see from this figure, the key rate of the untrusted detector noise scenario drops quickly at a short distance less than 20 km even though the electronic noise is only 0.01 SNU, which is a low value compared to detectors used in many other CV experiments. On the other hand, the key rate in the trusted detector noise scenario extends to much longer distances, which exhibits a similar behavior as the results shown in Ref. [31] when the detector is treated as ideal. One explanation for this behavior is that in Ref. [31], we observe that the key rate for the QPSK scheme drops quickly when the channel excess noise ξ is large. Since the value of ξ is reported at the input of the quantum channel while the value of ν_{el} is measured at

Bob's side, to treat ν_{el} as a part of channel excess noise in the untrusted detector noise scenario, one needs to define the effective value of ξ to include the value of ν_{el}. For the effective value ξ_{eff}, the electronic noise ν_{el} needs to be scaled by a factor of $1/\eta_t$ (in addition to $1/\eta_d$), which is large for slightly long distances as η_t becomes small. As a result, the redefined value ξ_{eff} of ξ is quite large as shown in Fig. 3 and this behavior of key rate is then expected. By the observation made from this figure, it is not surprised that for a larger value of electronic noise, the key rate in the untrusted detector noise scenario would drop to zero at an even shorter distance.

B. Detector imperfection in the trusted detector noise scenario

To guide the experimental implementation of the QPSK scheme, we may be interested in the robustness of the protocol in the presence of detector inefficiency and electronic noise in the trusted detector noise scenario. For this purpose, we investigate the effects of different levels of detector efficiency and electronic noise on the key rate. For curves in Figs. 4 and 5, our simulation uses the same channel model but different detector imperfections, that is, in Eq. (26), the same values of channel parameters η_t and ξ but different values of detector efficiency η_d and electronic noise ν_{el} (as specified in the captions) for different curves.

In Fig. 4, we choose values of η_d and ν_{el} for a homodyne detector from two experiments [12,14] and compare these results with the ideal detector. For the comparison, we optimize α via a coarse-grained search for each distance. We
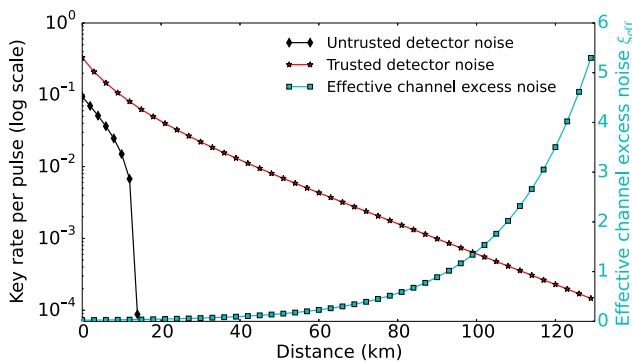

FIG. 3. Secure key rate versus the transmission distance for untrusted detector noise (black diamonds) and trusted detector noise (red stars) scenarios. The excess noise is $\xi = 0.01$ at the input of the quantum channel. Parameters for detector are $\eta_d = 0.719$, $\nu_{el} = 0.01$ [14]. The error-correction efficiency is $\beta = 0.95$. The coherent state amplitude is optimized via a coarse-grained search over the interval $[0.5, 0.9]$ with a step size of 0.05 and the channel transmittance is $\eta_t = 10^{-0.02L}$ for each distance L in kilometers. The effective channel excess noise in the untrusted detector scenario is shown with the y axis on the right. At 20 km, the effective channel excess noise ξ_{eff} is roughly 0.045.
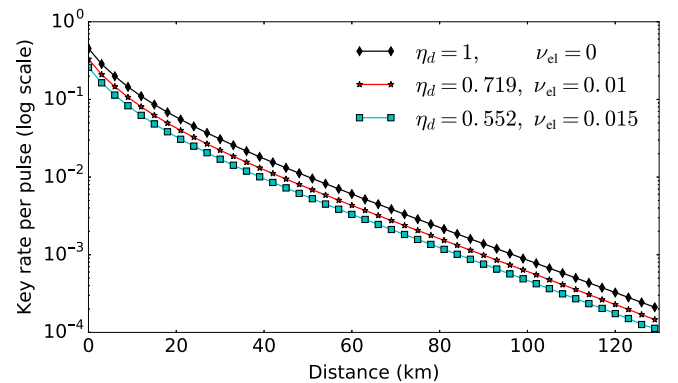

FIG. 4. Secure key rate versus transmission distance for different detector imperfections reported in experiments in a comparison to the ideal detector. Other parameters are the excess noise $\xi = 0.01$, error-correction efficiency $\beta = 0.95$, and the transmittance $\eta_t = 10^{-0.02L}$ for each distance L in kilometers. For each distance, the coherent-state amplitude α is optimized via a coarse-grained search in the interval $[0.5, 0.9]$ with a step size of 0.05. Black curve with diamond markers is for the ideal heterodyne detector; red curve with star markers is for the detector used in Ref. [14]; cyan curve with square markers is for the detector used in Ref. [12].
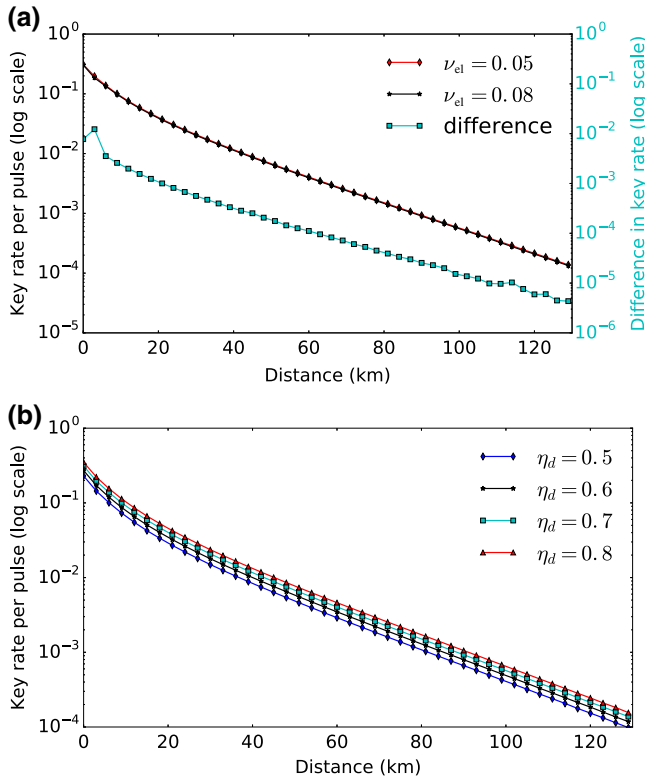
(a)

(b)

FIG. 5. Secure key rate versus transmission distance for different detector imperfections with the excess noise $\xi = 0.01$. For both plots, the coherent-state amplitude is optimized via a coarse-grained search over the interval $[0.5, 0.9]$ with a step size 0.05 and $\beta = 0.95$. (a) Comparison of key rates between two values of the electronic noise when the detector efficiency is set to be $\eta_d = 0.7$ for both curves. The difference of two curves is also plotted with the secondary y axis on the right. (b) Comparison of key rates for different values of detector efficiency when the electronic noise is $\nu_{el} = 0.05$.

see that with a noisy heterodyne detector, the key rate drops moderately from the key rate of using an ideal detector. The amount of decrease is like a constant prefactor in the key rate. As the detector is noisier, the key rate becomes lower as expected.

To show that different values of electronic noise have little impacts on the secure key rates in the trusted noise scenario, we compare key rates with two choices of the electronic noise value in Fig. 5(a) while we fix the value of detector efficiency η_d to be 0.7. As the key-rate difference is relatively small between the curve with $\nu_{el} = 0.05$ and that with $\nu_{el} = 0.08$, we also plot the difference of key rate (that is, the key rate with $\nu_{el} = 0.05$ minus the key rate with $\nu_{el} = 0.08$) in the same figure. (Note that the nonsmoothness in the curve of difference is due to the coarse-grained search for the coherent state amplitude in the presence of the numerical performance issue discussed in Ref. [31].) We observe that when the electronic noise is trusted, its impact on the secure key rates is insignificant. This result eases the requirements of a detector in a CVQKD
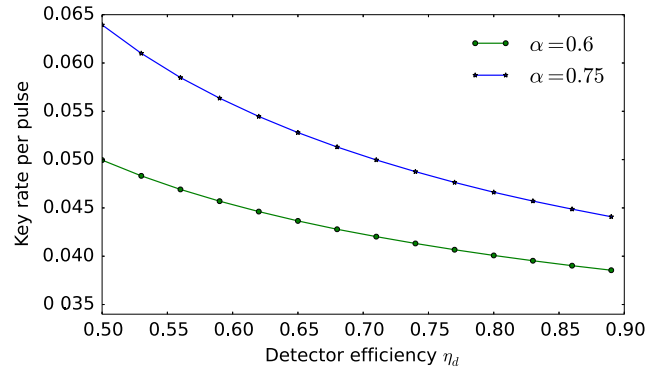

FIG. 6. Secure key rate versus the detector efficiency η_d for a fixed value of total transmittance $\eta := \eta_t \eta_d = 0.3155$. This figure studies the trade-off between the key rate and the amount of trusted loss. Other parameters are the excess noise $\xi = 0.01$, the electronic noise $\nu_{el} = 0.01$, and the error-correction efficiency $\beta = 0.95$. We include two curves for different choices of coherent-state amplitude α.

experiment with the QPSK scheme. Similarly, we investigate the effects of detector efficiency in Fig. 5(b). In particular, we fix the value of electronic noise ν_{el} to be 0.05 SNU and plot four choices of detector efficiency between 0.5 and 0.8. We see the key-rate curves are close to each other.

In Fig. 6, we investigate the trade-off between trusting the detector efficiency and lumping it together with the channel transmittance, similar to a scenario studied in Ref. [53] for discrete-variable systems. For the fixed amount of total transmittance $\eta := \eta_t \eta_d$, it is interesting to see how trusting different values of detector efficiency affects the key rate. We observe that when the value of the product of channel transmittance η_t and detector efficiency η_d is fixed, if the detector efficiency η_d is lower, meaning that if more contribution to the total transmittance η is trusted, then the key rate is higher. This observation is similar to the observation made for discrete-variable systems in Ref. [53].

To summarize, in a discrete modulation experiment, if one is able to obtain accurate values of η_d and ν_{el} by a suitable calibration procedure and able to maintain a low level of the effective channel excess noise ξ to a value like 0.01, then the QPSK scheme is able to extend to a distance beyond 100 km in the asymptotic regime. We remark that the optimal amplitude for the QPSK scheme in the trusted detector noise scenario is around 0.75 corresponding to a mean photon number of around 0.56, similar to the optimal amplitude in the ideal or untrusted detector noise scenario reported in our previous work [31]. This mean photon number is much lower than that for Gaussian modulation schemes.

VII. KEY RATE WITH POSTSELECTION

In this section, we investigate the effects of postselection in the trusted detector noise scenario. As demonstrated
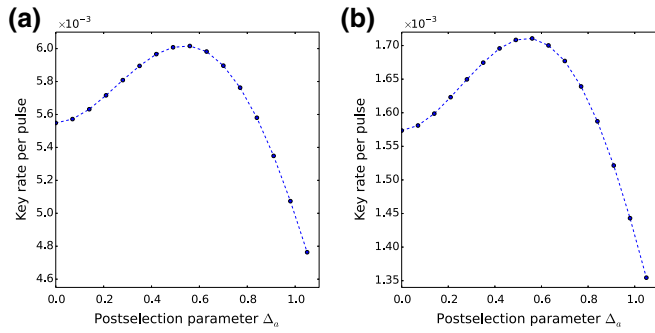
FIG. 7. (a) Secure key rate versus postselection parameter Δ_a for $L = 50$ km. (b) Secure key rate versus postselection parameter Δ_a for $L = 75$ km. For both plots, the channel excess noise is $\xi = 0.01$ and the error-correction efficiency $\beta = 0.95$. The coherent state amplitude is optimized via a coarse-grained search in the interval [0.6, 0.8] with a step size of 0.05. Parameters for detectors are $\eta_d = 0.552$ and $\nu_{el} = 0.015$ from Ref. [12].
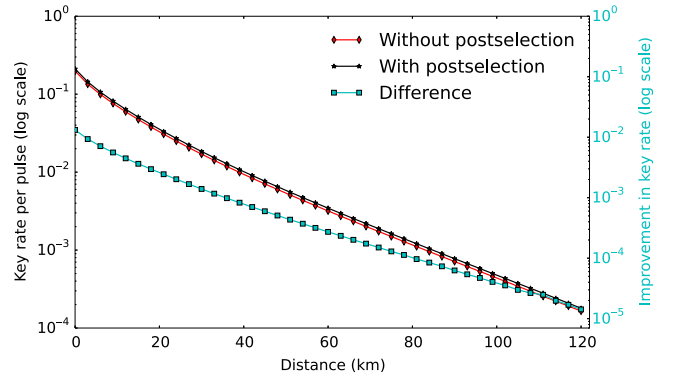
FIG. 8. Comparison of key rates with or without postselection. Detector parameters are from Ref. [12] where $\eta_d = 0.552$ and $\nu_{el} = 0.015$. The difference of two curves is also plotted with the secondary y axis on the right. Other parameters are the channel excess noise $\xi = 0.01$, the coherent-state amplitude $\alpha = 0.75$, and the error-correction efficiency $\beta = 0.95$. The postselection parameter is optimized via a coarse-grained search in the interval [0.45,0.7] with a step size 0.05.

in our previous analysis [31], postselection of data can improve the key rate of the QPSK scheme in the untrusted detector noise scenario. Postselection is simple to implement in an experiment. It not only improves the key rate but also reduces the required volume of data postprocessing. Thus, it is advantageous to include a postselection step in the protocol. As expected, we show here that this advantage also exists in the trusted detector noise scenario.

In Fig. 7, we search for the optimal postselection parameter for different transmission distances and take the distances $L = 50$ km and $L = 75$ km as examples. For this figure, we also optimize the choice of coherent-state amplitude via a coarse-grained search. The x axis in each plot is the postselection parameter Δ_a. We observe the optimal value of the postselection parameter Δ_a is around 0.6 for both $L = 50$ km and $L = 75$ km. We also observe that the optimal choice of the postselection parameter Δ_a does not change significantly for different distances.

In Fig. 8, we show the key rate as a function of transmission distance for two scenarios: with or without postselection. Since the optimal postselection parameter does not change significantly for different distances, we optimize the postselection parameter Δ_a via a coarse-grained search in a restricted interval. For this figure, we fix the coherent state amplitude to be 0.75 and the channel excess noise ξ to be 0.01. We see postselection can indeed improve the key rate. The percentage of improvement compared to the key rate without postselection is roughly between 5% to 8% and the probability of being postselected is around 70% to 80%. Thus, postselection can reduce the amount of data for postprocessing by around 20% to 30% while improving the key rate.

We end this section with a remark on the postselection pattern. The postselection pattern (see Fig. 1) studied in this work is a simple, intuitive, and convenient choice

when we evaluate the region operators. However, it is not necessarily the optimal way to postselect data [8,54]. It is an interesting future work to investigate other patterns of postselection.

VIII. SUMMARY AND FUTURE DIRECTIONS

We provide a method to analyze the asymptotic security of a discrete modulation scheme of CVQKD in the trusted detector noise scenario where both nonunity detector efficiency and electronic noise are trusted. In particular, we find the POVM elements corresponding to a noisy heterodyne detector. As we demonstrate our method on the quadrature phase-shift keying scheme, we show that when the detector imperfection is trusted, the key rates are similar to the one with the ideal heterodyne detector studied previously [31]. Our analysis in this work eases the requirements of an experimental implementation of the discrete modulation scheme as the detector imperfection is usually a major source of noise.

We point out the limitations in the current work. First, the analysis in this work is still restricted to the asymptotic scenario. We notice that there is a recent work on the finite-key analysis of binary modulation protocol [55]. However, the key rate there was very pessimistic and one expects that quadrature-shift keying schemes will have much better performance. It remains an open question to provide a finite-key analysis of general discrete modulation beyond binary modulation. As we recently extend the underlying numerical method used in this security analysis to finite-key regime [40], we hope to perform the finite-key analysis for discrete modulation schemes, especially the protocol

studied in this work. However, there remain technical challenges to solve before such an analysis can be carried out and thus we leave the finite-key analysis for future work. The second limitation is the same photon-number cutoff assumption used in Refs. [30,31]. While numerical evidences show that our results are stable when the cutoff photon number is chosen appropriately, we plan to have a more rigorous analysis on the effects of truncation beyond numerical evidences in future work. Thirdly, we present simulation results in a simple scenario where two homodyne components are treated as identical. This scenario is commonly assumed in previous studies of Gaussian modulation schemes. In the simple scenario, we are able to provide simplified expressions for region operators and observables used in the key-rate optimization problem. However, our principles presented in this paper work for the general case where two detectors are not identical. To handle the general case, one may perform the numerical integration of POVM element G_y's to find necessary operators in the photon-number basis from the photon-number basis representation of each POVM element G_y shown in Appendix B 2. It may become numerically demanding to perform these integrals. Alternatively, one may attempt to simplify expressions analytically similar to what we have done for the simple case. It remains as a technical question to efficiently compute the matrix elements of operators defined in terms of G_y in the photon-number basis, which we expect can be solved. Nevertheless, this current limitation does not affect the principles and methodology we present in this work about the treatment of trusted detector noise. It is also expected that observations in the general case will be similar to observations we make here in the simple case.

Finally, we remark on the generality of our method of treating trusted detector noise. If a different physical model of a detector is adopted (which needs to be verified experimentally), we expect that a similar method as described here can be used to find a correct POVM description for the given physical model and then this POVM can be used in the security analysis.

APPENDIX A: DERIVATION OF NOISY HETERODYNE DETECTION POVM VIA WIGNER FUNCTIONS

1. Basic Wigner functions

As we use the Wigner function approach for our derivation, we recall useful expressions from Ref. [56] for later references.

To calculate $\mathrm{Tr}(FG)$ for two operators F and G in terms of their Wigner functions W_F and W_G, the overlap formula is

$$\mathrm{Tr}(FG) = \pi \int d^2\alpha \, W_F(\alpha) W_G(\alpha). \tag{A1}$$

We can easily generalize the formula to multimode cases. The input-output Wigner functions under a beam-splitter transformation whose transmittance is η are related by

$$W_{\mathrm{out}}(\alpha, \beta) = W_{\mathrm{in}}(\sqrt{\eta}\alpha + \sqrt{1-\eta}\beta, \sqrt{1-\eta}\alpha - \sqrt{\eta}\beta). \tag{A2}$$

We list Wigner functions of some quantum states that are relevant for our discussions here. The Wigner function of a vacuum state $|0\rangle$ is

$$W_{|0\rangle}(\gamma) = \frac{2}{\pi} e^{-2|\gamma|^2}. \tag{A3}$$

The Wigner function of a thermal state $\rho_{\mathrm{th}}(\bar{n})$ with the mean photon number $\bar{n}$ is

$$W_{\rho_{\mathrm{th}}(\bar{n})}(\gamma) = \frac{2}{\pi} \frac{1}{1+2\bar{n}} e^{-2|\gamma|^2/(1+2\bar{n})}. \tag{A4}$$

The Wigner function of a displaced thermal state (DTS) $\rho_{\mathrm{DTS}}(\alpha, \bar{n}) := \hat{D}(\alpha)\rho_{\mathrm{th}}(\bar{n})\hat{D}^\dagger(\alpha)$ with the amount of displacement α is

$$W_{\rho_{\mathrm{DTS}}(\alpha,\bar{n})}(\gamma) = \frac{2}{\pi} \frac{1}{1+2\bar{n}} e^{-2|\gamma-\alpha|^2/(1+2\bar{n})}. \tag{A5}$$

We notice that if we set $\alpha = 0$, it reduces to Eq. (A4).

It is also useful to note the Wigner functions of a squeezed thermal state (STS) and of a displaced squeezed thermal state (DSTS). Let $\hat{S}(\xi)$ denote the squeezing operator with a squeezing parameter ξ. For our discussion, we restrict $\xi \in \mathbb{R}$. For a squeezed thermal state $\rho_{\mathrm{STS}}(\xi, \bar{n}) := \hat{S}(\xi)\rho_{\mathrm{th}}(\bar{n})\hat{S}^\dagger(\xi)$, its Wigner function reads [see, e.g., Eq. (4.13) of Ref. [57]]

$$\begin{aligned} W_{\rho_{\mathrm{STS}}(\xi,\bar{n})}(\gamma) &= \frac{2}{\pi} \frac{1}{1+2\bar{n}} \\ &\times \exp\left\{ -2\left[\frac{e^{2\xi}\mathrm{Re}(\gamma)^2 + e^{-2\xi}\mathrm{Im}(\gamma)^2}{1+2\bar{n}} \right] \right\}. \end{aligned} \tag{A6}$$

The Wigner function of a displaced squeezed thermal state $\rho_{\mathrm{DSTS}}(\alpha, \xi, \bar{n}) := \hat{D}(\alpha)\hat{S}(\xi)\rho_{\mathrm{th}}(\bar{n})\hat{S}^\dagger(\xi)\hat{D}^\dagger(\alpha)$ can be
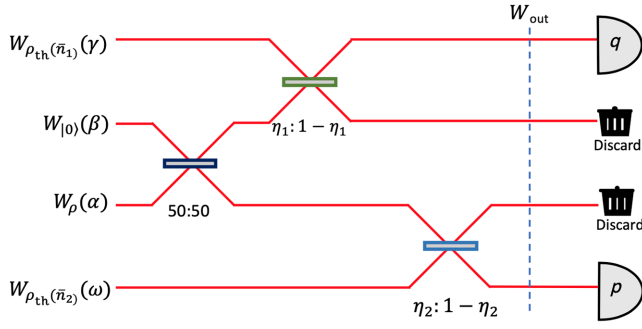
FIG. 9. A concise but equivalent view of the noisy heterodyne detector model depicted in Fig. 2. Input modes are labeled in terms of Wigner functions.

similarly written as

$$
W_{\rho_{\mathrm{DSTS}}(\alpha,\xi,\bar{n})}(\gamma) = \frac{2}{\pi}\frac{1}{1+2\bar{n}}
$$

$$
\times \exp\left\{-2\left[\frac{e^{2\xi}\mathrm{Re}(\gamma-\alpha)^2 + e^{-2\xi}\mathrm{Im}(\gamma-\alpha)^2}{1+2\bar{n}}\right]\right\}.
$$

$$(A7)$$

2. Derivation

As the physical model of a noisy heterodyne detector is presented in Fig. 2, our goal here is to find the corresponding POVM elements that correctly produce the probability density function $P(y)$ of obtaining an outcome $y \in \mathbb{C}$ for an arbitrary input state ρ to the detector. In our trusted noise model, the homodyne detector for the q quadrature measurement has its detector efficiency η_1 and electronic noise ν_1, which is related to a thermal state of the mean photon number $\bar{n}_1 = \nu_1/[2(1-\eta_1)]$. Similarly, the homodyne detector for the p quadrature measurement has its detector efficiency η_2 and electronic noise ν_2, which corresponds to a thermal state with the mean photon number $\bar{n}_2 = \nu_2/[2(1-\eta_2)]$. Figure 9 shows a compact but equivalent representation of Fig. 2 with Wigner functions associated to input modes. In this setup, for an output state $W_{\mathrm{out}}(\alpha,\beta,\gamma,\omega)$ at the step labeled in Fig. 9, we

measure the q quadrature of the mode α and p quadrature of the mode β with two ideal homodyne detectors, and discard the rest modes γ and ω. The Wigner function of an ideal homodyne detector for the q quadrature measurement that produces a measurement outcome $\mathrm{Re}(y)$ is $W_{H_{\mathrm{Re}(y)}}(\alpha) = [1/(\sqrt{2}\pi)]\delta(\mathrm{Re}(\alpha) - \mathrm{Re}(y)/\sqrt{2})$ where δ is the Dirac delta function and similarly, the one for the p quadrature measurement with a measurement outcome $\mathrm{Im}(y)$ is $W_{H_{\mathrm{Im}(y)}}(\alpha) = [1/(\sqrt{2}\pi)]\delta(\mathrm{Im}(\alpha) - \mathrm{Im}(y)/\sqrt{2})$. The factors of $\sqrt{2}$ are included such that we can rederive the ideal heterodyne detector POVM $\{E_y : y \in \mathbb{C}\}$ in the limit of unity detector efficiency and zero electronic noise. To discard modes γ and ω that are not measured, we perform the integration over variables γ and ω.

For any input state ρ to the detector, one can in principle obtain the underlying probability density function $P(y) = \mathrm{Tr}(\rho G_y)$ for every measurement outcome $y \in \mathbb{C}$. As the correct POVM element G_y needs to produce the observed probability density function $P(y) = \mathrm{Tr}(\rho G_y)$, this requirement in terms of Wigner functions becomes $P(y) = \pi \int d^2\alpha W_\rho(\alpha) W_{G_y}(\alpha)$, where W_ρ is the Wigner function of the input state ρ and W_{G_y} is the Wigner function of the operator G_y, by the overlap formula in Eq. (A1). In Fig. 9, we know the mathematical description of measurements on the right, but the description of the state W_{out} is unknown. On the other hand, we want to find the description of the measurement directly acting on the input state and the Wigner function description of the input state and those of ancillary modes on the left are either assumed to be given or known. To connect these known descriptions on the two sides of this diagram to find the desired Wigner function of the POVM element G_y that acts on the input state directly, we start from the right-hand side of this diagram with an unknown four-mode state W_{out} and the known measurements on these modes, perform inverse beam-splitter transformations from right to left of this diagram and finally obtain W_{G_y} by integrating over variables other than α. By starting with the multimode overlap formula for $P(y)$ on the right-hand side of the diagram and performing the process as described, we obtain

$$
P(y) = \pi^4 \int d^2\alpha \int d^2\beta \int d^2\gamma \int d^2\omega \frac{1}{\pi^2} W_{\mathrm{out}}(\alpha,\beta,\gamma,\omega) W_{H_{\mathrm{Re}(y)}}(\alpha) W_{H_{\mathrm{Im}(y)}}(\beta)
$$

$$
= \pi^2 \int d^2\alpha\, W_\rho(\alpha) \int d^2\beta W_{|0\rangle}(\beta) \int d^2\gamma\, W_{\rho_{\mathrm{th}}(\bar{n}_1)}(\gamma) W_{H_{\mathrm{Re}(y)}}\left(\sqrt{\eta_1}\frac{\alpha+\beta}{\sqrt{2}} + \sqrt{1-\eta_1}\gamma\right)
$$

$$
\times \int d^2\omega W_{\rho_{\mathrm{th}}(\bar{n}_2)}(\omega) W_{H_{\mathrm{Im}(y)}}\left(\sqrt{\eta_2}\frac{\alpha-\beta}{\sqrt{2}} + \sqrt{1-\eta_2}\omega\right).
$$

$$(A8)$$

The next step is to substitute the Wigner function of the vacuum state in Eq. (A3) and that of the thermal state in Eq. (A4) and then to perform the integrals over variables β, γ, and ω. We first integrate over the variable ω. The relevant integral that involves the variable ω is

$$\int d^2\omega\, W_{\rho_{\text{th}}(\bar{n}_2)}(\omega) W_{H_{\text{Im}(y)}}\left(\sqrt{\eta_2}\frac{\alpha - \beta}{\sqrt{2}} + \sqrt{1 - \eta_2}\omega\right)$$

$$= \frac{1}{\pi\sqrt{\pi}}\frac{1}{\sqrt{(1 - \eta_2)(1 + 2\bar{n}_2)}}$$

$$\times \exp\left\{-\frac{\eta_2[\text{Im}(\beta) + \frac{1}{\sqrt{\eta_2}}\text{Im}(y) - \text{Im}(\alpha)]^2}{(1 + 2\bar{n}_2)(1 - \eta_2)}\right\}. \quad \text{(A9)}$$

Next, we perform the integral related to the variable γ. Since Eq. (A9) does not involve the variable γ, we do not need to plug it back to solve the integral that involves the variable γ. This integration shown in Eq. (A10) is actually similar to the integration that we just did in Eq. (A9).

$$\int d^2\gamma\, W_{\rho_{\text{th}}(\bar{n}_1)}(\gamma) W_{H_{\text{Re}(y)}}\left(\sqrt{\eta_1}\frac{\alpha + \beta}{\sqrt{2}} + \sqrt{1 - \eta_1}\gamma\right)$$

$$= \frac{1}{\pi\sqrt{\pi}}\frac{1}{\sqrt{(1 - \eta_1)(1 + 2\bar{n}_1)}}$$

$$\times \exp\left\{-\frac{\eta_1[\text{Re}(\beta) - \frac{1}{\sqrt{\eta_1}}\text{Re}(y) + \text{Re}(\alpha)]^2}{(1 + 2\bar{n}_1)(1 - \eta_1)}\right\}. \quad \text{(A10)}$$

Finally, we integrate over the variable β. We now need to substitute results of Eqs. (A9) and (A10) back to Eq. (A8). The prefactor is simplified to be $(1/\pi^3)[1/\sqrt{(1 - \eta_1)(1 + 2\bar{n}_1)(1 - \eta_2)(1 + 2\bar{n}_2)}]$. Except this prefactor, we perform the following integral:

$$\int d^2\beta\, W_{|0\rangle}(\beta) \exp\left\{-\frac{\eta_1\left[\text{Re}(\beta) - \frac{1}{\sqrt{\eta_1}}\text{Re}(y) + \text{Re}(\alpha)\right]^2}{(1 + 2\bar{n}_1)(1 - \eta_1)}\right\} \exp\left\{-\frac{\eta_2\left[\text{Im}(\beta) + \frac{1}{\sqrt{\eta_2}}\text{Im}(y) - \text{Im}(\alpha)\right]^2}{(1 + 2\bar{n}_2)(1 - \eta_2)}\right\}$$

$$= 2\sqrt{\frac{(1 + 2\bar{n}_1)(1 + 2\bar{n}_2)(1 - \eta_1)(1 - \eta_2)}{[1 + (1 - \eta_1) + 4\bar{n}_1(1 - \eta_1)][1 + (1 - \eta_2) + 4\bar{n}_2(1 - \eta_2)]}}$$

$$\times \exp\left\{\frac{-2\eta_1\left[\frac{1}{\sqrt{\eta_1}}\text{Re}(y) - \text{Re}(\alpha)\right]^2}{1 + (1 - \eta_1) + 4\bar{n}_1(1 - \eta_1)} + \frac{-2\eta_2\left[\frac{1}{\sqrt{\eta_2}}\text{Im}(y) - \text{Im}(\alpha)\right]^2}{1 + (1 - \eta_2) + 4\bar{n}_2(1 - \eta_2)}\right\}. \quad \text{(A11)}$$

Finally, by putting the prefactor back and expressing the final expression in a format of Gaussian functions, we obtain the following result:

$$W_{G_y}(\alpha) = \frac{1}{\sqrt{\eta_1\eta_2}\pi}\frac{2}{\pi}\frac{1}{\sqrt{1 + \frac{2(1-\eta_1)(1+2\bar{n}_1)}{\eta_1}}}\frac{1}{\sqrt{1 + \frac{2(1-\eta_2)(1+2\bar{n}_2)}{\eta_2}}}$$

$$\times \exp\left\{\frac{-2\left[\frac{1}{\sqrt{\eta_1}}\text{Re}(y) - \text{Re}(\alpha)\right]^2}{1 + \frac{2(1-\eta_1)(1+2\bar{n}_1)}{\eta_1}} + \frac{-2\left[\frac{1}{\sqrt{\eta_2}}\text{Im}(y) - \text{Im}(\alpha)\right]^2}{1 + \frac{2(1-\eta_2)(1+2\bar{n}_2)}{\eta_2}}\right\}. \quad \text{(A12)}$$

By substituting in $\bar{n}_1 = \nu_1/[2(1 - \eta_1)]$ and $\bar{n}_2 = \nu_2/[2(1 - \eta_2)]$, we derive Eq. (12) after a straightforward simplification.

3. POVM elements

a. General case

As we derive the Wigner function of an arbitrary POVM element G_y corresponding to the detector model in Fig. 2, we next show that the POVM elements G_y's are projections onto displaced squeezed thermal states up to a scaling factor. To see this, we make the following definitions:

$$\lambda_j := \frac{(1 - \eta_j)(1 + 2\bar{n}_j)}{\eta_j} = \frac{1 - \eta_j + \nu_j}{\eta_j} \quad \text{for } j = 1, 2,$$

$$\bar{n}_{\text{het}} := \frac{\sqrt{(1 + 2\lambda_1)(1 + 2\lambda_2)} - 1}{2},$$

$$\xi_{\text{het}} := \frac{1}{4}\ln\left[\frac{1 + 2\lambda_2}{1 + 2\lambda_1}\right],$$

$$\alpha_{\text{het}} := \frac{1}{\sqrt{\eta_1}}\text{Re}(y) + \frac{i}{\sqrt{\eta_2}}\text{Im}(y). \quad \text{(A13)}$$

With these choices of parameters $\alpha_{\text{het}}, \xi_{\text{het}}$, and $\bar{n}_{\text{het}}$, Eq. (A12) can be rewritten as

$$W_{G_y}(\gamma) = \frac{1}{\sqrt{\eta_1 \eta_2} \pi} \frac{2}{\pi} \frac{1}{1 + 2\bar{n}_{\text{het}}} \exp\left\{-2\left[\frac{e^{2\xi_{\text{het}}} \text{Re}(\gamma - \alpha_{\text{het}})^2 + e^{-2\xi_{\text{het}}} \text{Im}(\gamma - \alpha_{\text{het}})^2}{1 + 2\bar{n}_{\text{het}}}\right]\right\}. \tag{A14}$$

By comparing the Wigner function of G_y in Eq. (A12) and the Wigner function of a displaced squeezed thermal state in Eq. (A7), we can identify $G_y = [1/(\sqrt{\eta_1 \eta_2}\pi)]\rho_{\text{DSTS}}(\alpha_{\text{het}}, \xi_{\text{het}}, \bar{n}_{\text{het}})$ for the choices of parameters $\alpha_{\text{het}}, \xi_{\text{het}}$, and $\bar{n}_{\text{het}}$ in Eq. (A13). Therefore, each G_y is a scaled projection onto a displaced squeezed thermal state with the displacement α_{het}, squeezing parameter ξ_{het} and the mean photon number of the initial thermal state before squeezing and displacement $\bar{n}_{\text{het}}$.

b. Simple case

If $\eta_1 = \eta_2 = \eta_d$ and $\nu_1 = \nu_2 = \nu_{\text{el}}$, it is easy to verify that Eq. (A12) reduces to Eq. (13). Then one can identify each POVM element G_y is the projection onto a displaced thermal state with a prefactor $1/(\eta_d\pi)$ in Eq. (14). An alternative view is to look at the parameters $\alpha_{\text{het}}, \xi_{\text{het}}$, and $\bar{n}_{\text{het}}$ in Eq. (A13). In particular, since $\lambda_1 = \lambda_2$, the amount of squeezing ξ_{het} becomes zero. Thus, by neglecting squeezing in the POVM elements of the general case, one can also conclude each POVM element is proportional to the projection onto a displaced thermal state. One can further verify that the displacement is $\alpha_{\text{het}} = y/\sqrt{\eta_d}$ and the mean photon number of the initial thermal state $\bar{n}_{\text{het}}$ becomes $(1 - \eta_d + \nu_{\text{el}})/\eta_d$.

APPENDIX B: PHOTON-NUMBER BASIS REPRESENTATION OF OPERATORS

In this appendix, we show how to represent region operators as well as observables needed for the optimization problem in Eq. (22) in the photon-number basis. By the same discussion in Appendix B of Ref. [31], under the photon-number cutoff assumption, we need only to find $\Pi_N \hat{O} \Pi_N$ for an operator $\hat{O}$ with a cutoff photon number N. Thus, we are interested in finding the expression $\langle m| \hat{O} |n\rangle$ for $0 \le m, n \le N$ for each relevant operator $\hat{O}$. When these operators are represented in this finite-dimensional Hilbert space spanned by $\{|n\rangle : 0 \le n \le N\}$, we can then proceed with numerical optimization to calculate the key rate.

In Appendix B 1, our discussion is restricted to the simplified scenario that we use in the main text for presenting simulation results; that is, we set $\eta_1 = \eta_2 = \eta_d$ and $\nu_1 = \nu_2 = \nu_{\text{el}}$. Under this scenario, we present formulae that can be efficiently evaluated in MATLAB. We then discuss the general case where the imperfections in two homodyne detectors are not necessarily the same in Appendix B 2. For the general case, we provide the matrix representation of the POVM elements G_y's and leave the evaluation

of region operators and observables for the optimization problem to be done numerically.

1. Simple case

In this simple case where two homodyne detectors in the heterodyne detection scheme have the same imperfection, the POVM element G_y given in Eq. (14) in the photon-number basis is expressed as [48]

$$\langle m| G_y |n\rangle = \frac{1}{\eta_d\pi} \exp\left[-\frac{|y|^2}{\eta_d(1 + \bar{n}_d)}\right] \frac{\bar{n}_d^m}{(1 + \bar{n}_d)^{n+1}}$$
$$\times \left(\frac{y^*}{\sqrt{\eta_d}}\right)^{n-m} \left(\frac{m!}{n!}\right)^{1/2}$$
$$\times L_m^{(n-m)}\left[-\frac{|y|^2}{\eta_d\bar{n}_d(1 + \bar{n}_d)}\right], \tag{B1}$$

where we define $\bar{n}_d = (1 - \eta_d + \nu_{\text{el}})/\eta_d$ for ease of writing and $L_k^{(j)}(x)$ is the generalized Laguerre polynomial of degree k with a parameter j in the variable x. In particular, the diagonal entries are simplified to be

$$\langle n| G_y |n\rangle = \frac{1}{\eta_d\pi} \exp\left[-\frac{|y|^2}{\eta_d(1 + \bar{n}_d)}\right]$$
$$\times \frac{\bar{n}_d^n}{(1 + \bar{n}_d)^{n+1}} L_n\left[-\frac{|y|^2}{\eta_d\bar{n}_d(1 + \bar{n}_d)}\right], \tag{B2}$$

where $L_k(x) = L_k^{(0)}(x)$ is the Laguerre polynomial of degree k in the variable x. For ease of writing later, we define $C_{m,n} = [1/(\pi \eta_d^{(n-m)/2+1})](m!/n!)^{1/2}[\bar{n}_d^m/(1 + \bar{n}_d)^{n+1}]$.

a. Region operators

Our goal here is to write region operators $R_j = \int_{y \in \mathcal{A}_j} G_y d^2y$ in the photon-number basis. For simplicity, we work out the expressions in the absence of postselection. To include the postselection, one may numerically integrate over the discarded region and subtract this result from the expression without postselection since this numerical integration is efficiently computable in MATLAB. We first consider off-diagonal elements (i.e., $m \ne n$). In this case, we plug the expression of $\langle m| G_y |n\rangle$ in Eq. (B1) into the definition of R_j in Eq. (16), write it in the polar coordinate with $y = re^{i\theta}$ and perform the integration over the phase θ to obtain the following expression:

$$\langle m | R_j | n \rangle = \int_0^\infty dr\, r \int_{(2j-1)\pi/4}^{(2j+1)\pi/4} d\theta\, \langle m | G_{re^{i\theta}} | n \rangle$$

$$= C_{m,n} \frac{i[e^{i(m-n)(2j-1)\pi/4} - e^{i(m-n)(2j+1)\pi/4}]}{m-n} \int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(n-m)}\left[-\frac{r^2}{\eta_d \bar{n}_d(1+\bar{n}_d)}\right] r^{n-m+1}. \quad \text{(B3)}$$

Performing the integral over the variable r, we obtain the result in terms of Taylor series expansion of a simple function:

$$\int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(n-m)}\left[-\frac{r^2}{\eta_d \bar{n}_d(1+\bar{n}_d)}\right] r^{n-m+1}$$

$$= \frac{1}{2}[\eta_d(1+\bar{n}_d)]^{[(n-m)/2]+1} \Gamma\left(\frac{n-m}{2}+1\right) f_m\left(\bar{n}_d, n-m, \frac{n-m}{2}\right), \quad \text{(B4)}$$

where Γ is the gamma function and $f_m(a,\alpha,k)$ is defined as the Taylor series coefficients of the function below in the variable t as

$$(1-t)^{-\alpha+k}\left[1-\left(1+\frac{1}{a}\right)t\right]^{-(k+1)} = \sum_{n=0}^\infty f_n(a,\alpha,k) t^n. \quad \text{(B5)}$$

We note that the Taylor series coefficients here can be quickly found in MATLAB.

Now, we consider the diagonal entries of R_j (i.e., $m=n$). By substituting $y = re^{i\theta}$ in Eq. (B2), we note that this expression does not depend on θ. Thus, it is easy to see $\langle n| R_0 |n\rangle = \langle n| R_1 |n\rangle = \langle n| R_2 |n\rangle = \langle n| R_3 |n\rangle$. The integration over the phase θ gives a factor of $\pi/2$. We proceed the integration over variable r and obtain

$$\langle n| R_j |n\rangle = \frac{\pi}{2}\frac{1}{\eta_d \pi}\int_0^\infty dr\, r \exp\left[-\frac{r^2}{\eta(1+\bar{n}_d)}\right]\frac{\bar{n}_d^n}{(1+\bar{n}_d)^{n+1}} L_n\left[-\frac{r^2}{\eta_d \bar{n}_d(1+\bar{n}_d)}\right]$$

$$= \frac{1}{4}\frac{\bar{n}_d^n}{(1+\bar{n}_d)^n}\left(1+\frac{1}{\bar{n}_d}\right)^n = \frac{1}{4}. \quad \text{(B6)}$$

To include postselection, the common integral in the case $m \neq n$ becomes

$$\int_{\Delta_a}^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(n-m)}\left[-\frac{r^2}{\eta_d \bar{n}_d(1+\bar{n}_d)}\right] r^{n-m+1}$$

$$= \frac{1}{2}[\eta_d(1+\bar{n}_d)]^{[(n-m)/2]+1}\Gamma\left(\frac{n-m}{2}+1\right) f_m\left(\bar{n}_d, n-m, \frac{n-m}{2}\right)$$

$$- \int_0^{\Delta_a} dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(n-m)}\left[-\frac{r^2}{\eta_d \bar{n}_d(1+\bar{n}_d)}\right] r^{n-m+1}, \quad \text{(B7)}$$

where the second term is efficiently computable numerically. The case for $m=n$ follows similarly.

b. First-moment observables

We then proceed to evaluate the matrix elements of $\hat{F}_Q$ and $\hat{F}_P$. In the photon-number basis, the matrix elements are

$$\langle m| \hat{F}_Q |n\rangle = \int \frac{y+y^*}{\sqrt{2}} \langle m| G_y |n\rangle\, d^2y$$

$$= \frac{C_{m,n}}{\sqrt{2}}\int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(n-m)}\left[-\frac{r^2}{\eta_d \bar{n}_d(1+\bar{n}_d)}\right] r^{n-m+2}\int_0^{2\pi} d\theta\, e^{-i(n-m)\theta}(e^{i\theta}+e^{-i\theta}),$$

$$\langle m| \hat{F}_P |n\rangle = \int \frac{i(y^*-y)}{\sqrt{2}} \langle m| G_y |n\rangle\, d^2y$$

$$= \frac{iC_{m,n}}{\sqrt{2}}\int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(n-m)}\left[-\frac{r^2}{\eta_d \bar{n}_d(1+\bar{n}_d)}\right] r^{n-m+2}\int_0^{2\pi} d\theta\, e^{-i(n-m)\theta}(e^{-i\theta}-e^{i\theta}). \quad \text{(B8)}$$

As $\hat{F}_Q$ is a Hermitian operator, we can first find entries $\langle m| \hat{F}_Q |n\rangle$ for $m \leq n$. Then for $m > n$, we simply set $\langle m| \hat{F}_Q |n\rangle$ to be the complex conjugate of $\langle n| \hat{F}_Q |m\rangle$. From the integration over θ, the nonzero entries for $m \leq n$ are

$$
\begin{aligned}
\langle m| \hat{F}_Q |m+1\rangle &= \sqrt{2}\pi C_{m,m+1} \int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(1)}\left(-\frac{r^2}{\eta_d\bar{n}_d(1+\bar{n}_d)}\right) r^3 \\
&= \frac{\pi}{\sqrt{2}} C_{m,m+1}[(1+\bar{n}_d)\eta_d]^2 f_m(\bar{n}_d,1,1).
\end{aligned}
\tag{B9}
$$

By a similar procedure for $\hat{F}_P$, we have

$$
\begin{aligned}
\langle m| \hat{F}_P |m+1\rangle &= -\sqrt{2}i\pi C_{m,m+1} \int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(1)}\left[-\frac{r^2}{\eta_d\bar{n}_d(1+\bar{n}_d)}\right] r^3 \\
&= -\frac{i\pi}{\sqrt{2}} C_{m,m+1}[(1+\bar{n}_d)\eta_d]^2 f_m(\bar{n}_d,1,1).
\end{aligned}
\tag{B10}
$$

c. Second-moment observables

Next, we evaluate the matrix elements of $\hat{S}_Q$ and $\hat{S}_P$. In the photon-number basis, they are

$$
\begin{aligned}
\langle m| \hat{S}_Q |n\rangle &= \int \left(\frac{y+y^*}{\sqrt{2}}\right)^2 \langle m| G_y |n\rangle d^2 y \\
&= \frac{C_{m,n}}{2} \int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(n-m)}\left(-\frac{r^2}{\eta_d\bar{n}_d(1+\bar{n}_d)}\right) r^{n-m+3} \int_0^{2\pi} d\theta\, e^{-i(n-m)\theta}(e^{i\theta}+e^{-i\theta})^2, \\
\langle m| \hat{S}_P |n\rangle &= \int \left(\frac{i(y^*-y)}{\sqrt{2}}\right)^2 \langle m| G_y |n\rangle d^2 y \\
&= -\frac{C_{m,n}}{2} \int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(n-m)}\left[-\frac{r^2}{\eta_d\bar{n}_d(1+\bar{n}_d)}\right] r^{n-m+3} \int_0^{2\pi} d\theta\, e^{-i(n-m)\theta}(e^{-i\theta}-e^{i\theta})^2.
\end{aligned}
\tag{B11}
$$

Again, since $\hat{S}_Q$ and $\hat{S}_P$ are Hermitian operators, we only need to define the upper triangular part and then set the lower triangular part using the Hermitian property. The relevant integrals are simplified to be

$$
\begin{aligned}
\langle m| \hat{S}_Q |m\rangle &= 2\pi C_{m,m} \int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m\left[-\frac{r^2}{\eta_d\bar{n}_d(1+\bar{n}_d)}\right] r^3 \\
&= \pi C_{m,m}[\eta_d(1+\bar{n}_d)]^2 f_m(\bar{n}_d,0,1), \\
\langle m| \hat{S}_Q |m+2\rangle &= \pi C_{m,m+2} \int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(2)}\left[-\frac{r^2}{\eta_d\bar{n}_d(1+\bar{n}_d)}\right] r^5 \\
&= \pi C_{m,m+2}[\eta_d(1+\bar{n}_d)]^3 f_m(\bar{n}_d,2,2).
\end{aligned}
\tag{B12}
$$

For $\hat{S}_P$, we have

$$
\begin{aligned}
\langle m| \hat{S}_P |m\rangle &= 2\pi C_{m,m} \int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m\left[-\frac{r^2}{\eta_d\bar{n}_d(1+\bar{n}_d)}\right] r^3 \\
&= \pi C_{m,m}[\eta_d(1+\bar{n}_d)]^2 f_m(\bar{n}_d,0,1), \\
\langle m| \hat{S}_P |m+2\rangle &= -\pi C_{m,m+2} \int_0^\infty dr \exp\left[-\frac{r^2}{\eta_d(1+\bar{n}_d)}\right] L_m^{(2)}\left[-\frac{r^2}{\eta_d\bar{n}_d(1+\bar{n}_d)}\right] r^5 \\
&= -\pi C_{m,m+2}[\eta_d(1+\bar{n}_d)]^3 f_m(\bar{n}_d,2,2).
\end{aligned}
\tag{B13}
$$

2. General case

We consider the general case where two homodyne detectors may have different imperfections. In this case, each POVM element G_y is given in Eq. (A14). Given the POVM $G_y = [1/(\sqrt{\eta_1 \eta_2}\pi)]\rho_{\text{DSTS}}(\alpha_{\text{het}}, \xi_{\text{het}}, \bar{n}_{\text{het}})$, its matrix elements are given by Eq. (5.2) of Ref. [58] with the prefactor $1/(\sqrt{\eta_1 \eta_2}\pi)$ as

$$\langle m| G_y |n\rangle = \frac{1}{\sqrt{\eta_1 \eta_2}} \frac{Q(0)}{\sqrt{m!n!}} \sum_{k=0}^{\min(m,n)} k! \binom{m}{k}\binom{n}{k}\tilde{A}^k$$
$$\times \left(\frac{\tilde{B}}{2}\right)^{(m-k)/2} \left(\frac{\tilde{B}^*}{2}\right)^{(n-k)/2}$$
$$\times H_{m-k}[(2\tilde{B})^{-1/2}\tilde{C}]H_{n-k}[(2\tilde{B}^*)^{-1/2}\tilde{C}^*], \tag{B14}$$

where H_ℓ is the Hermite polynomial of order ℓ. With simple substitutions, one may verify that these parameters $\tilde{A}, \tilde{B}, \tilde{C}$, and $Q(0)$ are defined in terms of $\lambda_1, \lambda_2, \alpha_{\text{het}}$ in Eq. (A13) as

$$\tilde{A} := 1 - \frac{\lambda_1 + \lambda_2 + 2}{2(\lambda_1 + 1)(\lambda_2 + 1)},$$
$$\tilde{B} := \frac{-|\lambda_1 - \lambda_2|}{2(\lambda_1 + 1)(\lambda_2 + 1)},$$
$$\tilde{C} := \frac{\text{Re}(\alpha_{\text{het}})}{\max(\lambda_1, \lambda_2) + 1} + i\frac{\text{Im}(\alpha_{\text{het}})}{\min(\lambda_1, \lambda_2) + 1},$$
$$Q(0) := \frac{1}{\pi} \frac{1}{\sqrt{(\lambda_1 + 1)(\lambda_2 + 1)}}$$
$$\times \exp\left[-\frac{\text{Re}(\alpha_{\text{het}})^2}{\max(\lambda_1, \lambda_2) + 1} - \frac{\text{Im}(\alpha_{\text{het}})^2}{\min(\lambda_1, \lambda_2) + 1}\right]. \tag{B15}$$

As indicated in Eqs. (5.3) and (5.4) of Ref. [58], the choice of square roots of $\tilde{B}$ is as $\tilde{B}^{1/2} = ie^{i(\varphi/2)}|\tilde{B}|^{1/2}$ and $(\tilde{B}^*)^{1/2} = (\tilde{B}^{1/2})^*$, where $\varphi = 0$ if $\lambda_1 \leq \lambda_2$ and $\varphi = \pi$ if $\lambda_1 > \lambda_2$. We note that $\bar{n}_{\text{het}}$ and ξ_{het} are defined in terms of λ_1 and λ_2 and one may rewrite these parameters in terms of $\bar{n}_{\text{het}}, \xi_{\text{het}}$, and α_{het} to make the matrix elements more explicitly depend on the parameters of the displaced squeezed thermal states.

From the expression of $\langle m| G_y |n\rangle$ in Eq. (B14), one can apply the definition of region operators R_j's in Eq. (16) to find $\langle m| R_j |n\rangle$ by numerical integration. Similarly, from the definitions of first- and second-moment observables in Eq. (21) in terms of POVM elements G_y's, one can numerically obtain a representation of these operators in the photon-number basis.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE international conference on computers, systems and signal processing* (IEEE, New York, 1984), p. 175.

[2] A. K. Ekert, Quantum Cryptography based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] 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).

[4] E. Diamanti and A. Leverrier, Distributing secret keys with quantum continuous variables: Principle, security and implementations, Entropy **17**, 6072 (2015).

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

[6] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in Quantum Cryptography, arXiv:1906.01645 (2019).

[7] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[8] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit, Phys. Rev. Lett. **89**, 167901 (2002).

[9] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using gaussian-modulated coherent states, Nature **421**, 238 (2003).

[10] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum Cryptography without Switching, Phys. Rev. Lett. **93**, 170504 (2004).

[11] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Quantum key distribution over 25 km with an all-fiber continuous-variable system, Phys. Rev. A **76**, 042305 (2007).

[12] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics **7**, 378 (2013).

[13] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution based on Coherent Detection, Phys. Rev. X **5**, 041009 (2015).

[14] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-Referenced Continuous-Variable Quantum Key Distribution Protocol, Phys. Rev. X **5**, 041010 (2015).

[15] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, High-speed continuous-variable quantum key distribution without sending a local oscillator, Opt. Lett. **40**, 3695 (2015).

[16] D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).

[17] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-Distance Continuous-Variable Quantum Key Distribution Over 202.81 km of Fiber, Phys. Rev. Lett. **125,** 010502 (2020).

[18] C. Wittmann, J. Fürst, C. Wiechers, D. Elser, H. Häseler, N. Lütkenhaus, and G. Leuchs, Witnessing effective entanglement over a 2 km fiber channel, Opt. Express **18,** 4499 (2010).

[19] X.-Y. Wang, Z.-L. Bai, S.-F. Wang, Y.-M. Li, and K.-C. Peng, Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise, Chin. Phys. Lett. **30,** 010305 (2013).

[20] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, Atmospheric continuous-variable quantum communication, New J. Phys. **16,** 113018 (2014).

[21] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru, Implementation of continuous-variable quantum key distribution with discrete modulation, Quantum Sci. Technol. **2,** 024010 (2017).

[22] F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, F. Karinou, A. Poppe, M. Peev, and H. Hübel, Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator, Quantum **3,** 193 (2019).

[23] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5,** 5235 (2014).

[24] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8,** 15043 (2017).

[25] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security Against Coherent Attacks, Phys. Rev. Lett. **109,** 100502 (2012).

[26] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Analysis of imperfections in practical continuous-variable quantum key distribution, Phys. Rev. A **86,** 032309 (2012).

[27] E. Kaur, S. Guha, and M. M. Wilde, Asymptotic Security of Discrete-Modulation Protocols for Continuous-Variable Quantum Key Distribution, arXiv:1901.10099 (2019).

[28] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks, Phys. Rev. A **79,** 012307 (2009).

[29] K. Brádler and C. Weedbrook, Security proof of continuous-variable quantum key distribution using three coherent states, Phys. Rev. A **97,** 022310 (2018).

[30] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation, Phys. Rev. X **9,** 021059 (2019).

[31] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution, Phys. Rev. X **9,** 041064 (2019).

[32] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers, J. Phys. B **42,** 114014 (2009).

[33] V. C. Usenko and R. Filip, Trusted noise in continuous-variable quantum key distribution: A threat and a defense, Entropy **18,** 20 (2016).

[34] F. Laudenbach and C. Pacher, Analysis of the trusted-device scenario in continuous-variable quantum key distribution, Adv. Quantum Technol. **2,** 1900055 (2019).

[35] M. Navascués, F. Grosshans, and A. Acín, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97,** 190502 (2006).

[36] R. García-Patrón and N. J. Cerf, Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97,** 190503 (2006).

[37] R. Namiki, A. Kitagawa, and T. Hirano, Secret key rate of a continuous-variable quantum-key-distribution scheme when the detection process is inaccessible to eavesdroppers, Phys. Rev. A **98,** 042319 (2018).

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

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

[40] I. George, J. Lin, and N. Lütkenhaus, Numerical Calculations of Finite Key Rate for General Quantum Key Distribution Protocols, arXiv:2004.11865 (2020).

[41] In our previous work [31], we also considered a postselection parameter Δ_p related to the phase of the measurement outcome. However, when we perform simulations with this postselection parameter, we do not obtain any noticeable advantage. Thus, we omit the introduction of this parameter in this work.

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

[43] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables, Quantum Inf. Comput. **3,** 535 (2003).

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

[45] 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).

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

[47] The electronic noise ν_j is the thermal noise added by the detection electronics. In the quantum-mechanical model of the detector shown in each dashed box of Fig. 2, the electronic noise is modeled by an ancillary thermal state added to the second input port of the beam splitter that models the detector efficiency. Since the value of electronic noise is unaffected by the detector efficiency, to simulate the desired amount of noise before this beam splitter, one then needs

to scale it by the reflectance of the beam splitter, which is $1 - \eta_j$. As the variance of a thermal state with a mean photon number $\bar{n}$ is $(1 + 2\bar{n})N_0$, one can easily see that the mean photon number of this ancillary thermal state is $\bar{n}_j = v_j/[2(1 - \eta_j)]$.

[48] B. R. Mollow and R. J. Glauber, Quantum theory of parameteric amplification. I, Phys. Rev. **160**, 1076 (1967).

[49] K. E. Cahill and R. J. Glauber, Ordered expansions in boson amplitude operators, Phys. Rev. **177**, 1857 (1969).

[50] K. E. Cahill and R. J. Glauber, Density operators and quasiprobability distributions, Phys. Rev. **177**, 1882 (1969).

[51] Due to our definition of quadrature operators, we include the factor $\sqrt{2}$ so that we can simply enter values reported in an experiment using shot-noise units as expectation values of corresponding observables.

[52] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography, npj Quantum Inf. **4**, 21 (2018).

[53] Y. Zhang, P. J. Coles, A. Winick, J. Lin, and N. Lütkenhaus, Security Proof of Practical Quantum Key Distribution with Detection-Efficiency Mismatch, arXiv:2004.04383 (2020).

[54] M. Heid and N. Lütkenhaus, Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction, Phys. Rev. A **73**, 052316 (2006).

[55] T. Matsuura, K. Maeda, T. Sasaki, and M. Koashi, Finite-Size Security of Continuous-Variable Quantum Key Distribution with Digital Signal Processing, arXiv:2006.04661 (2020).

[56] U. Leonhardt, *Essential Quantum Optics: from Quantum Measurements to Black Holes* (Cambridge University Press, Cambrige, England, 2010).

[57] M. S. Kim, F. A. M. de Oliveira, and P. L. Knight, Properties of squeezed number states and squeezed thermal states, Phys. Rev. A **40**, 2494 (1989).

[58] P. Marian and T. A. Marian, Squeezed states with thermal noise. I. Photon-number statistics, Phys. Rev. A **47**, 4474 (1993).