1-15-2021

Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution

Eneet Kaur
Louisiana State University

Saikat Guha
The University of Arizona

Mark M. Wilde
Louisiana State University

Recommended Citation

Kaur, E., Guha, S., & Wilde, M. (2021). Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Physical Review A, 103* (1) https://doi.org/10.1103/PhysRevA.103.012412

Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution

Eneet Kaur,[1] Saikat Guha,[2] and Mark M. Wilde[1]

[1] *Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, and Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA*

[2] *College of Optical Sciences and Department of Electrical and Computer Engineering, University of Arizona, Tucson, Arizona 85719, USA*

(Dated: January 20, 2021)

We consider discrete-modulation protocols for continuous-variable quantum key distribution (CV-QKD) that employ a modulation constellation consisting of a finite number of coherent states and that use a homodyne or a heterodyne-detection receiver. We establish a security proof for collective attacks in the asymptotic regime, and we provide a formula for an achievable secret-key rate. Previous works established security proofs for discrete-modulation CV-QKD protocols that use two or three coherent states. The main constituents of our approach include approximating a complex, isotropic Gaussian probability distribution by a finite-size Gauss-Hermite constellation, applying entropic continuity bounds, and leveraging previous security proofs for Gaussian-modulation protocols. As an application of our method, we calculate secret-key rates achievable over a lossy thermal bosonic channel. We show that the rates for discrete-modulation protocols approach the rates achieved by a Gaussian-modulation protocol as the constellation size is increased. For pure-loss channels, our results indicate that in the high-loss regime and for sufficiently large constellation size, the achievable key rates scale optimally, i.e., proportional to the channel's transmissivity.

I. INTRODUCTION

Quantum key distribution (QKD) allows for two distant parties, often called Alice and Bob, to create a shared secret key by employing an insecure and noisy quantum communication channel and an authenticated public classical communication channel [1–3]. The security is based on the physical laws of quantum mechanics, in contrast to conventional cryptographic protocols, whose security relies on computational complexity-theoretic assumptions.

There are two basic classes of QKD protocols that have been considered: discrete-variable and continuous-variable (see, e.g., [3] for a review). In discrete-variable QKD (DV-QKD), the information is usually encoded in the polarization or time bin of single photons or weak coherent states (laser-light pulses). Discrete-variable QKD requires high-efficiency, low dark-count-rate, single-photon detectors, which are expensive and often need extreme cryo-cooling. In the other class of protocols, known as continuous-variable QKD (CV-QKD), the information is encoded in the quadrature amplitudes of coherent states. The transmitter modulates the phase and/or the amplitude of laser-light pulses, and the receiver is based on coherent detection (i.e., homodyne or heterodyne detection). Near shot-noise-limited, low-noise homodyne/heterodyne detection is readily realizable at room temperature using off-the-shelf hardware, unlike the single-photon detectors of DV-QKD. CV-QKD protocols thus possess a major advantage over DV-QKD in terms of the cost and ease of experimental implementation.

However, one major area that DV-QKD currently possesses an advantage over CV-QKD is that the DV modulation involves few levels (e.g., two polarization states of a photon or three amplitude levels of a coherent state in the decoy-state BB84 protocol [4–6]), which puts far less burden on the transmitter's modulator compared to that of the traditional Gaussian-modulation CV-QKD protocol. The latter requires modulation using an infinite-size constellation. This also makes the error correction protocols far simpler for DV-QKD, along with much less overhead for random-number generation. Another area where DV-QKD is arguably more advanced is the availability of quantum repeater protocols [7–11] for overcoming the fundamental rate-vs.-loss trade-off of direct-transmission based QKD [12–14]. However, there have been recent advances in designs of repeaters for CV-QKD [15–17]. For experimental developments in CV-QKD see [18–23].

In the most common form of CV-QKD, one uses Gaussian modulation of coherent states [24]: Alice modulates laser-light pulses with amplitudes selected randomly from a complex-valued Gaussian distribution with a given variance. Security proofs for this Gaussian modulation CV-QKD protocol have been developed for arbitrary attacks, even in the finite key-length regime [25]. Additionally, a suite of variants of this CV-QKD protocol exist, some of which use squeezed light modulation and two-way transmission [26–34].

However, all of their asymptotic security proofs require a Gaussian modulation. Gaussian modulation has obvious drawbacks, which include extreme burden on the transmitter's random number source, as well as computationally demanding and inefficient error-correction techniques. Furthermore, no matter how high the extinction ratio of a practically-realizable electro-optic modulator, it is impossible to sample pulse amplitudes from a true Gaussian distribution, on which the security proofs rely.

Despite the fact that Gaussian modulation has made security proofs manageable, it is important—for the prac-

tical realizability of CV-QKD—that protocols that use a few pre-determined modulation levels (such as binary phase and quadrature amplitude modulation) are proven secure. Discrete-modulation CV-QKD was introduced in [35–37], where the coherent states transmitted in each mode are chosen according to a discrete probability distribution, and it was developed further in [38]. Discrete-modulation CV-QKD protocols can leverage the efficient modulation and error correction, and low-overhead random number generation that DV-QKD enjoys, while retaining the ease of implementation of homodyne/heterodyne detection of CV-QKD.

Several discrete-modulation protocols have already been considered [38–41], and security proofs have been developed in the asymptotic regime, i.e., in the limit of a large number of uses of the quantum channel, hence generating a large-length key (at a given key-bits per channel-use rate). Ref. [38] considered a protocol with binary-phase shift-keying of coherent states along with homodyne detection. However, the secure key rate established there is more than an order of magnitude lower than that which can be achieved with Gaussian modulation. Motivated by [38], Ref. [39] considered ternary-phase shift-keying modulation with homodyne detection, which led to an improvement in the secure key rates, but the resulting secret-key rates are still far from the key rates achievable with Gaussian modulation. Refs. [40, 41] established security for discrete-modulation protocols against particular collective attacks that correspond to linear bosonic channels. For other protocols that use discrete modulation of coherent states, see [42, 43].

This brings us to the long-standing open problem of proving security of a general M-ary discrete-modulation CV-QKD protocol, for M beyond a minimum threshold value, with the feature that the achievable key rate approaches that of Gaussian modulation as M goes to infinity. Such a result is of significant value for the practical usability of CV-QKD. In this paper, we accomplish the aforesaid for security against collective attacks having the physically reasonable assumptions outlined in Section III. Establishing a security proof and key-rate lower bounds for discrete modulation CV-QKD protocols with a finite key length is left open for future work. Our proof eliminates the need to consider protocols based on Gaussian modulation in order to have asymptotic security in CV-QKD, with the ability of the user to determine the size of the modulation alphabet based on how close one desires the key rates to be to the Gaussian modulation protocol. In addition, our numerical evaluation of achievable key rates over a pure-loss bosonic channel suggests that, for sufficiently large constellation size, the achievable key rates are proportional to the channel's transmissivity, which is known to be the optimal rate-vs.-loss scaling achievable with any QKD protocol, CV or DV [12].

To establish these results, we make use of two important recent theoretical advances: the approximation of Gaussian distributions with discrete ones for communication [44, 45], especially in the context of bosonic Gaussian states [45], and an entropic continuity bound from [46] for energy-bounded bosonic states. The idea of approximating a Gaussian modulation with a discrete one for CV-QKD was proposed in [47], but this work did not provide a security proof for CV-QKD with discrete modulation. One of the main tools, beyond the approaches considered in [47] and which allows us to establish a security proof, is the entropic continuity bound from [46]. We also develop methods for using the parameters observed in a discrete-modulation CV-QKD protocol to bound Eve's Holevo information.

This paper is organized as follows. We introduce discrete-modulation CV-QKD in Section II, followed by Section III's detailed list of our assumptions on the collective attack of an eavesdropper. We give our security proof in Section IV, and we discuss details of channel estimation in Section V. We then showcase, in Section VI, the secure key rates that our approach leads to when the protocol is conducted over a lossy thermal bosonic channel. We end with open questions and future directions in Section VII.

Note: In work independent of and concurrent to ours, other approaches for security proofs in discrete modulation of CV-QKD have been put forward [48, 49].

II. PROTOCOL

We begin by outlining the steps of a phase-symmetrized discrete-modulation CV-QKD protocol based on m^2 coherent states, where $m \in \mathbb{N}$. In this protocol, Bob performs either homodyne or heterodyne detection. Let X be a random variable with realizations $x \in \{1, 2, \ldots, m^2\}$ and fix $\alpha_x \in \mathbb{C}$ for all x. Let $r(x)$ be the probability associated with the realization x. The steps of the protocol are as follows:

1. Alice prepares the coherent state $|\alpha_x\rangle$ with probability $r(x)$. She records the value of x in the variable x_j, where $j \in \{1, \ldots, n\}$ refers to the transmission round. She also records the value $\sqrt{2}\,\mathrm{Re}\{\alpha_x\}$ in the variable q_j and the value $\sqrt{2}\,\mathrm{Im}\{\alpha_x\}$ in the variable p_j . Exact expressions for α_x and $r(x)$ that we use in the protocol are given in Section V.

2. Alice then picks a phase $\phi_j \in \{0, \pi/2, \pi, 3\pi/2\}$ uniformly at random, applies it to her channel input mode as the unitary $e^{-i\hat{n}\phi_j}$, which is physically realized by a phase shifter. The resulting state is then $e^{-i\hat{n}\phi_j}|\alpha_x\rangle = |\alpha_x e^{-i\phi_j}\rangle$, which she transmits over the unknown and insecure quantum communication channel $\mathcal{N}$ to Bob. At the same time, she communicates the choice ϕ_j to Bob over a public authenticated classical channel and then she locally discards or forgets the choice of ϕ_j. The insecure quantum channel $\mathcal{N}$ can be controlled by an eavesdropper Eve. Our assumptions on the insecure quantum channel $\mathcal{N}$ are stated in Section III.

3. Upon receiving the output of the quantum channel, namely, the state $\mathcal{N}(e^{-i\hat{n}\phi_j}|\alpha_x\rangle\langle\alpha_x|e^{i\hat{n}\phi_j})$, as well as the classical choice of ϕ_j from the public authenticated classical channel, Bob applies the reverse phase as the inverse unitary $e^{i\hat{n}\phi_j}$, and then locally discards or forgets the value of ϕ_j. The resulting state is then as follows:

$$\overline{\mathcal{N}}(|\alpha_x\rangle\langle\alpha_x|), \tag{1}$$

where the phase-symmetrized channel $\overline{\mathcal{N}}$ is defined as

$$\overline{\mathcal{N}}(\rho) \equiv \frac{1}{4}\sum_{k=0}^{3} U(k)^\dagger \mathcal{N}(U(k)\rho U(k)^\dagger)U(k), \tag{2}$$

with $U(k) \equiv e^{-i\hat{n}\pi k/2}$. The phase symmetrization of the channel $\mathcal{N}$ is helpful in reducing the number of parameters that need to be estimated during the channel estimation part of the protocol, as we explain in Section V.

4. If Bob performs position-quadrature or real-quadrature homodyne detection on the state $\overline{\mathcal{N}}(|\alpha_x\rangle\langle\alpha_x|)$ the result is recorded in the variable y_j^q [50]. If Bob performs heterodyne detection, then the value of the position quadrature is recorded in y_j^q, and the value of the momentum quadrature is recorded in y_j^p.

5. Steps 1-4 are repeated n times, for n a large positive integer. If Bob performs homodyne detection, then the sequence $\{q_j\}_{j=1}^n$ is known to Alice, and the sequence $\{y_j^q\}_{j=1}^n$ is known to Bob. If Bob performs heterodyne detection, then the sequences $\{q_j\}_{j=1}^n$ and $\{p_j\}_{j=1}^n$ are known to Alice, and $\{y_j^q\}_{j=1}^n$ and $\{y_j^p\}_{j=1}^n$ are known to Bob.

6. A constant fraction δ of the rounds are used for channel estimation (or parameter estimation), for $\delta \in (0,1)$ a small number. That is, for these δn rounds, the parameters γ_{11}, γ_{22}, and γ_{12} are calculated. If Bob performs homodyne detection, then these parameters are given as

$$\gamma_{11} \equiv \frac{1}{\delta n}\sum_{j=1}^{\delta n}(q_j - \overline{q})^2, \tag{3}$$

$$\gamma_{12} \equiv \frac{1}{\delta n}\sum_{j=1}^{\delta n}(q_j - \overline{q})(y_j^q - \overline{y}), \tag{4}$$

$$\gamma_{22} \equiv \frac{1}{\delta n}\sum_{j=1}^{\delta n}(y_j^q - \overline{y})^2, \tag{5}$$

where

$$\overline{q} \equiv \frac{1}{\delta n}\sum_{j=1}^{\delta n} q_j, \qquad \overline{y} \equiv \frac{1}{\delta n}\sum_{j=1}^{\delta n} y_j^q. \tag{6}$$

If Bob performs heterodyne detection, then these parameters are given as

$$\gamma_{11} \equiv \frac{1}{\delta n}\sum_{j=1}^{\delta n}(q_j - \overline{q})^2 = \frac{1}{\delta n}\sum_{j=1}^{\delta n}(p_j - \overline{p})^2, \tag{7}$$

$$\gamma_{12} \equiv \frac{1}{2\delta n}\sum_{j=1}^{\delta n}(q_j - \overline{q})(y_j^q - \overline{y}^q) + (p_j - \overline{p})(y_j^p - \overline{y}^p), \tag{8}$$

$$\gamma_{22} \equiv \frac{1}{2\delta n}\sum_{j=1}^{\delta n}(y_j^q - \overline{y}^q)^2 + (y_j^p - \overline{y}^p)^2, \tag{9}$$

where

$$\overline{q} \equiv \frac{1}{\delta n}\sum_{j=1}^{\delta n} q_j, \qquad \overline{y}^q \equiv \frac{1}{\delta n}\sum_{j=1}^{\delta n} y_j^q, \tag{10}$$

$$\overline{p} \equiv \frac{1}{\delta n}\sum_{j=1}^{\delta n} p_j, \qquad \overline{y}^p \equiv \frac{1}{\delta n}\sum_{j=1}^{\delta n} y_j^p. \tag{11}$$

Clearly, the parameter γ_{11} can be calculated from Alice's data alone, γ_{22} can be calculated from Bob's data alone, but it is necessary to calculate γ_{12} from both Alice and Bob's data, and so it is necessary for Bob to share the y_j values of these δn rounds with Alice over a public authenticated classical channel. Furthermore, the public authenticated classical channel is used for Alice and Bob to share the values of γ_{11}, γ_{12}, and γ_{22} with each other. The data x_j, q_j, p_j and $y_j^{q,p}$ for these δn channel estimation rounds are then discarded. A detailed analysis of the channel estimation part of the protocol is given in Section V.

7. The remaining q_j, p_j, and $y_j^{q,p}$ data are used for final key generation. The final key-generation protocol includes reverse reconciliation, error correction, and privacy amplification (see [3] for a review).

III. ASSUMPTIONS ON THE INSECURE QUANTUM COMMUNICATION CHANNEL

In this section, we outline the various assumptions that we make on the insecure quantum communication channel:

1. Each Alice-to-Bob transmission is assumed to take place over independent identical uses of a quantum channel $\mathcal{N}$, which is unknown to Alice and Bob at the beginning of the protocol. We assume that any deviation of $\mathcal{N}$ from the identity channel is attributed to the most general adversarial action by Eve. Even though Eve's action—which appears as a noisy quantum channel $\mathcal{N}$ to Alice and Bob—remains the same for each transmission, she is allowed to make arbitrary collective measurements

on her quantum system at the end of the protocol. See below for a mathematical description. This scenario is referred to as a *collective attack*.

2. The channel is described mathematically as an isometric quantum channel $\mathcal{U}_{A\to BE}$, meaning that there exists an isometry $U_{A\to BE}$, satisfying $[U_{A\to BE}]^\dagger U_{A\to BE} = I_A$, such that

$$\mathcal{U}_{A\to BE}(\rho_A) \equiv U_{A\to BE}\,\rho_A\,(U_{A\to BE})^\dagger \tag{12}$$

for all input density operators ρ_A. The systems A, B, and E are described by separable Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$, and $\mathcal{H}_E$, respectively. The system A corresponds to a single bosonic mode, and system B does also. In particular, the channel can accept coherent states at the input A and is such that the receiver can perform homodyne or heterodyne detection on the system B. The system A is accessible to the sender Alice, the system B is accessible to the receiver Bob, and the system E is in possession of the eavesdropper Eve.

3. The reduced channel from Alice to Bob is given by

$$\mathcal{N}_{A\to B}(\rho_A) \equiv \mathrm{Tr}_E[\mathcal{U}_{A\to BE}(\rho_A)], \tag{13}$$

and this channel $\mathcal{N}_{A\to B}$ is what is used in the protocol description in Section II. We assume that if the mean photon number of the input state ρ_A is finite, then the mean photon number of the output state $\mathcal{N}_{A\to B}(\rho_A)$ is finite. That is, $\mathrm{Tr}[\hat{n}\mathcal{N}_{A\to B}(\rho_A)] < \infty$ if $\mathrm{Tr}[\hat{n}\rho_A] < \infty$. Furthermore, we assume that if the variance of the photon number of the input state ρ_A is finite, then the variance of the photon number of the output state $\mathcal{N}_{A\to B}(\rho_A)$ is finite. This implies that $\mathrm{Tr}[\hat{n}^2\mathcal{N}_{A\to B}(\rho_A)] < \infty$ if $\mathrm{Tr}[\hat{n}^2\rho_A] < \infty$.

4. We assume that if the mean photon number of the input state ρ_A is finite, then the mean energy of Eve's state $\mathrm{Tr}_B[\mathcal{U}_{A\to BE}(\rho_A)]$ is finite, where the mean energy is computed with respect to a physically reasonable Hamiltonian H_E that satisfies the Gibbs hypothesis [51–53], meaning that $\mathrm{Tr}[e^{-\beta H_E}] < \infty$ for all $\beta > 0$ and has its ground-state energy equal to zero. For example, if Eve's system E of the state $\mathrm{Tr}_B[\mathcal{U}_{A\to BE}(\rho_A)]$ consists of several bosonic modes $E_1, \ldots, E_k$, then H_E could be taken as the total photon number operator $\hat{n}_1 + \cdots + \hat{n}_k$ for all of the k modes.

5. Let

$$\mu(q_A, p_A) \equiv \int dq_B\, r_{Q_B|Q_A,P_A}(q_B|q_A p_A)\, q_B, \tag{14}$$

denote the conditional mean of the position quadrature of Bob, where $r_{Q_B|Q_A,P_A}(q_B|q_A p_A)$ is the conditional probability distribution of the position quadrature q_B of the state

$$\sigma_B^{q_A,p_A} \equiv \mathcal{N}_{A\to B}(|\alpha(q_A,p_A)\rangle\langle\alpha(q_A,p_A)|_A), \tag{15}$$

and $|\alpha(q_A,p_A)\rangle\langle\alpha(q_A,p_A)|$ is a coherent state with position quadrature q_A and momentum quadrature p_A. We suppose that $\mu(q_A,p_A) = \sum_{k=0}^{K_1}\sum_{l=0}^{K_2}\mu_{kl}q_A^k p_A^l$, where $K_1, K_2 \in \mathbb{Z}^+$. That is, the mean value of the position quadrature of $\sigma_B^{q_A,p_A}$ is no more than a K_1th-order polynomial in q_A and a K_2th-order polynomial in p_A. We also suppose that μ_{kl} is an exponentially decaying function, $\exp[-a(k+l)]$, in k and l for $k \geq 2m-2$ and $l \geq 2m-1$. Here, $a > 0$ and m is the constellation size. For simplicity, we suppose that $K_1 = K_2$. These assumptions are required for the security proof presented in Appendix A.

We note that an immediate consequence of the bounded mean photon number assumption in part three above, by applying the Cauchy–Schwarz inequality, is the following: If Alice inputs a state ρ_A with finite mean vector $[\langle\hat{q}\rangle_\rho, \langle\hat{p}\rangle_\rho]$, then the output mean vector for the state of system B is finite. If the input state ρ_A has a finite covariance matrix with entries given by

$$\begin{bmatrix} 2\langle\hat{q}_0^2\rangle_\rho & \langle\hat{q}_0\hat{p}_0 + \hat{p}_0\hat{q}_0\rangle_\rho \\ \langle\hat{q}_0\hat{p}_0 + \hat{p}_0\hat{q}_0\rangle_\rho & 2\langle\hat{p}_0^2\rangle_\rho \end{bmatrix}, \tag{16}$$

where $\hat{q}_0 \equiv \hat{q} - \langle\hat{q}\rangle_\rho$ and $\hat{p}_0 \equiv \hat{p} - \langle\hat{p}\rangle_\rho$, then the covariance matrix of the output state $\mathcal{N}_{A\to B}(\rho_A)$ is finite.

IV. SECRET-KEY RATE LOWER BOUND

The asymptotic secret-key rate K is bounded from below by the Devetak-Winter formula [54, 55] as

$$K \geq I(X;Y) - \sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}} \chi(Y;E). \tag{17}$$

In the inequality above, the Shannon mutual information between Alice's variable X and Bob's variable Y is denoted by $I(X;Y)$, and the Holevo information between Bob's variable Y and Eve's quantum system E is denoted by $\chi(Y;E)$. We suppose that the quantum channel connecting Alice to Bob is not known, satisfies the assumptions given in Section III, and can only be partially estimated from X and the measurement outcomes Y on Bob's side, as we discuss in Section V. This lack of knowledge is an advantage to Eve. Therefore, the inequality in (17) features an optimization of the Holevo information $\chi(Y;E)$ over all isometric quantum channels $\mathcal{U}_{A\to BE}$ of Eve that are compatible with Alice's and Bob's data. Let $\mathcal{S}$ denote the set of channels that are consistent with the measurement data. We discuss the precise meaning of this statement in Section V. We also suppose that reverse reconciliation [56] is being used in the key-generation protocol, in which the public classical communication is from Bob to Alice, and this accounts for Bob's variable Y appearing in the $\chi(Y;E)$ term in (17).

To calculate the lower bound in (17), we first need to calculate the Shannon mutual information $I(X;Y)$,

which can be easily obtained from the observed data of Alice and Bob. The main difficulty is then to perform the optimization over the isometric quantum channels $\mathcal{U}_{A\to BE}$ of Eve and to bound the Holevo information $\chi(Y;E)$ from above. Doing so is the main bottleneck for many security proofs in quantum key distribution.

For protocols involving Gaussian modulation of coherent states, the aforementioned problem was solved in [57, 58], with [57] relying on the techniques of [59]. The optimal attack by Eve for such protocols was proved to be a Gaussian attack, which considerably simplifies the security analysis. However, once we consider discrete-modulation protocols, the optimal attack by Eve is no longer known, and is unlikely to be Gaussian. To address this problem, novel techniques are required.

In this paper, we provide a security proof for the protocol described in Section II by employing various existing tools: the approximation of Gaussian distributions with discrete ones [44, 45], an entropic continuity bound from [46], and the optimality of Gaussian attacks for Gaussian modulation of coherent states [57, 58]. The approach that we employ in this paper is rather intuitive: we approximate the Gaussian distribution with a discrete distribution and bound the error introduced due to this approximation in trace norm, by employing the techniques of [44, 45]. Then, we expect Eve's Holevo information due to this approximation to be close to Eve's Holevo information resulting from a Gaussian-modulated protocol, with the absolute value of the difference being a function of the error introduced in the approximation.

We now discuss this approach in detail. First, consider a key-generation protocol that employs coherent states with Gaussian modulation. The expected density operator for Alice's transmitted state is a thermal state $\theta(N_S)$ with mean photon number $N_S \geq 0$:

$$\theta(N_S) \equiv \frac{1}{N_S+1}\sum_{n=0}^{\infty}\left(\frac{N_S}{N_S+1}\right)^n |n\rangle\langle n|. \tag{18}$$

The P-function of the thermal state $\theta(N_S)$ is a circularly symmetric complex Gaussian [60]. Following the approach of [45], we can approximate the real and imaginary parts of the circularly symmetric Gaussian by the various constellations considered in [44]: Gauss-Hermite, random walk, equilattice, and quantile. The type of constellation fixes $|\alpha_x\rangle$ and $r(x)$. In this paper, we focus exclusively on the Gauss-Hermite constellation. It is possible to consider other constellations and obtain security proofs for these other constellations using the techniques described below. We obtain the error introduced by this approximation, by employing bounds from [45], and then we apply an entropic continuity bound from [46] to obtain an upper bound on Eve's Holevo information $\chi(Y;E)$.

We now discuss our security proof for discrete-modulation protocols of the form presented in Section II. Suppose that Alice employs the following discrete-modulation ensemble of coherent states:

$$\{r(x), |\alpha_x\rangle\}_{x=1}^{m^2}, \tag{19}$$

with expected density operator:

$$\overline{\rho} \equiv \sum_{x=1}^{m^2} r(x)|\alpha_x\rangle\langle\alpha_x|. \tag{20}$$

Then depending on the constellation size m^2 and the mean photon number N_S of the thermal state being approximated, we obtain the following bound on the normalized trace distance:

$$\frac{1}{2}\left\|\overline{\rho} - \theta(N_S)\right\|_1 \leq \varepsilon(m, N_S), \tag{21}$$

where $\theta(N_S)$ is a thermal state of mean photon number N_S and $\varepsilon(m, N_S)$ is the approximation error, for which we determine an explicit characterization later in (100), by employing the techniques of [45].

The secret-key rate with reverse reconciliation is given by

$$\beta I(X;Y) - \chi(Y;E), \tag{22}$$

where β is the reconciliation efficiency [61] and the mutual information quantities are computed with respect to the following ensemble:

$$\{r(x,y), \rho_E^{x,y}\}_{x,y}, \tag{23}$$

where

$$r(x,y) \equiv r(x)r(y|x), \tag{24}$$

$$r(y|x) \equiv \mathrm{Tr}\{(\Lambda_B^y \otimes I_E)\mathcal{U}_{A\to BE}(|\alpha_x\rangle\langle\alpha_x|_A)\}, \tag{25}$$

$$\rho_E^{x,y} \equiv \frac{1}{r(y|x)}\mathrm{Tr}_B\{(\Lambda_B^y \otimes I_E)\mathcal{U}_{A\to BE}(|\alpha_x\rangle\langle\alpha_x|_A)\}, \tag{26}$$

with $\{\Lambda^y\}_y$ denoting Bob's POVM and $\mathcal{U}_{A\to BE}$ the isometric channel satisfying the assumptions of Section III and corresponding to the collective attack of Eve. Since we do not know what collective attack Eve will employ, we minimize the secret-key rate with respect to all collective attacks that are consistent with the measurement data observed by Alice and Bob, i.e., with respect to all isometric channels $\mathcal{U}_{A\to BE}$ satisfying the assumptions of Section III and in the set $\mathcal{S}$. It is possible to estimate the Shannon mutual information $I(X;Y)$ from the measurement data of Alice and Bob, but we are left with the following optimization problem for Eve's Holevo information:

$$\sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}} \chi(Y;E)_{\mathcal{E}_\rho}, \tag{27}$$

where the optimization is with respect to all collective attacks of Eve consistent with the measurement data of Alice and Bob, and the subscript notation $\mathcal{E}_\rho$ indicates that the Holevo information $\chi(Y;E)$ between Bob's measurement outcome and Eve's quantum system is being computed with respect to the following ensemble:

$$\mathcal{E}_\rho \equiv \{r(y), \rho_E^y\}, \tag{28}$$

where

$$r(y) \equiv \sum_x r(x,y), \tag{29}$$

$$\begin{aligned}\rho_E^y &\equiv \sum_x r(x|y)\rho_E^{x,y} \\ &= \sum_x \frac{r(x|y)}{r(y|x)} \operatorname{Tr}_B\{(\Lambda_B^y \otimes I_E)\mathcal{U}_{A\to BE}(|\alpha_x\rangle\langle\alpha_x|_A)\} \\ &= \frac{1}{r(y)} \operatorname{Tr}_B\{(\Lambda_B^y \otimes I_E)\mathcal{U}_{A\to BE}(\overline{\rho}_A)\}.\end{aligned} \tag{30}$$

From the data processing inequality for trace distance (under the action of the isometric channel $\mathcal{U}_{A\to BE}$ and Bob's measurement channel), we find that

$$\begin{aligned}\varepsilon &\geq \frac{1}{2}\left\|\overline{\rho} - \theta(N_S)\right\|_1 \\ &\geq \frac{1}{2}\int dy \left\|r(y)\rho_E^y - r^G(y)\theta_E^y(N_S)\right\|_1,\end{aligned} \tag{31, 32}$$

where

$$r^G(y) \equiv \operatorname{Tr}\{(\Lambda_B^y \otimes I_E)\mathcal{U}_{A\to BE}(\theta(N_S))\}, \tag{33}$$

$$\theta_E^y(N_S) \equiv \frac{1}{r^G(y)} \operatorname{Tr}_B\{(\Lambda_B^y \otimes I_E)\mathcal{U}_{A\to BE}(\theta(N_S))\}. \tag{34}$$

We then define the following ensemble as that which would arise had Alice employed a Gaussian modulation at the channel input:

$$\mathcal{E}_\theta = \{r^G(y), \theta_E^y\}. \tag{35}$$

At this point, we invoke the fourth assumption from Section III: if the mean energy of the input state to the channel $\operatorname{Tr}_B \circ \mathcal{U}_{A\to BE}$ is fixed at some finite mean photon number $\kappa \in [0,\infty)$, then the mean energy of the output state is no larger than $\kappa'(\kappa) \in [0,\infty)$. Supposing that H_E is the Hamiltonian for Eve's system E satisfying the properties stated in the fourth assumption from Section III, by applying the continuity bound given in [46, Proposition 27], we find that

$$\chi(Y;E)_{\mathcal{E}_\rho} \leq \chi(Y;E)_{\mathcal{E}_\theta} + f(\varepsilon, P), \tag{36}$$

where P is an upper bound on the mean energy of the states $\operatorname{Tr}_B \circ \mathcal{U}_{A\to BE}(\overline{\rho}_A)$ and $\operatorname{Tr}_B \circ \mathcal{U}_{A\to BE}(\theta(N_S))$ and $f(\varepsilon, P)$ is a function of ε and P, given in [46], with the property that

$$\lim_{\varepsilon\to 0} f(\varepsilon, P) = 0. \tag{37}$$

In particular, the function $f(\varepsilon, P)$ is given by

$$\begin{aligned}f(\varepsilon, P) \equiv \varepsilon\,(2t + r_\varepsilon(t))\, S(\theta_E(P/\varepsilon t)) \\ + 2g(\varepsilon r_\varepsilon(t)) + 2h(\varepsilon t),\end{aligned} \tag{38}$$

for any $t \in (0, \frac{1}{2\varepsilon}]$, where

$$r_\varepsilon(t) \equiv (1 + t/2)/(1 - \varepsilon t), \tag{39}$$

$$g(x) \equiv (x+1)\log_2(x+1) - x\log_2(x), \tag{40}$$

$$h(x) \equiv -x\log_2(x) - (1-x)\log_2(1-x), \tag{41}$$

and $S(\theta_E(P/\varepsilon t))$ is the entropy of a thermal state $\theta_E(P/\varepsilon t)$ of Eve's system with mean energy $P/\varepsilon t$. Due to this uniform bound, we can then apply suprema to find that

$$\sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}} \chi(Y;E)_{\mathcal{E}_\rho} \leq \sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}} \chi(Y;E)_{\mathcal{E}_\theta} + f(\varepsilon, P), \tag{42}$$

with the optimizations again taken with respect to collective attacks of Eve consistent with the measurement data of Alice and Bob. The lower bound on the key rate is then given as

$$K \geq I(X;Y) - \sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}} \chi(Y;E)_{\mathcal{E}_\theta} - f(\varepsilon, P). \tag{43}$$

The Shannon mutual information between X and Y, i.e., the term $I(X;Y)$, can be calculated from the observed data, as mentioned previously. The term $f(\varepsilon, P)$, introduced due to the continuity of Holevo information, can be estimated from (38). Obtaining an upper bound on the remaining term, the Holevo information $\sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}} \chi(Y;E)_{\mathcal{E}_\theta}$, still requires further development, which we detail in the next section.

V. CHANNEL ESTIMATION

The main objective of this section is to obtain an upper bound on the remaining term, the Holevo information $\sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}} \chi(Y;E)_{\mathcal{E}_\theta}$. The approach that we take to obtain an upper bound can be divided into three parts: estimation of parameters from the actual protocol described in Section II, using these to bound the parameters that would result if a Gaussian-modulation protocol had been employed instead, and finally using these last estimates to bound the Holevo information $\sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}} \chi(Y;E)_{\mathcal{E}_\theta}$ from above.

A. Estimation of parameters from the actual discrete-modulation protocol

Alice and Bob calculate the parameters γ_{11}, γ_{12}, and γ_{22} given in (3)–(5) or in (7)–(9), depending on Bob's measurement, as described in Section II. Then the set $\mathcal{S}$ discussed in Section IV consists of all of the isometric channels $\mathcal{U}_{A\to BE}^{\mathcal{N}}$ that are consistent with the calculated values of γ_{11}, γ_{12}, and γ_{22}. In this way, Alice and Bob characterize the attack by Eve.

Since we are operating in the asymptotic regime, such that the number n of rounds is large, it follows that the number δn of channel estimation rounds is also large. Additionally, since Eve is employing a collective attack and the protocol has an i.i.d. structure, it follows that the parameters γ_{11}, γ_{12}, and γ_{22} are given exactly as the expectation of particular random variables.

To determine these random variables, we now give exact expressions for the constellation $\{\alpha_x\}_{x=1}^{m^2}$ and distribution $r_X(x)$ that are used in the protocol. We begin by recalling the Gauss-Hermite approximation to the normal distribution with zero mean and unit variance, which reproduces the first $2m-1$ moments of the Gaussian distribution [62, Section 3.6]. Let H_m be the mth Hermite polynomial, and let L_m be a random variable with m realizations l_{wm}, with probability distribution given by $r_{L_m}(l_{wm})$, where $w \in \{1,2,\ldots,m\}$. Then, as defined in [44], the values l_{wm} are set to the roots of the Hermite polynomial H_m, and the probability distribution $r_{L_m}(l_{wm})$ is defined as

$$r_{L_m}(l_{wm}) \equiv \frac{(m-1)!}{m H_{m-1}^2(l_{wm})}. \tag{44}$$

The P-function of a thermal state with mean photon number N_S is a circularly symmetric complex Gaussian [60]. Following [45], we approximate the real and imaginary parts of the thermal-state P-function individually by the constellation described above. Specifically, we choose q_{wm} for $w \in \{1,\ldots,m\}$ such that the sequence $\{q_{wm}/\sqrt{N_S}\}_w$ is equal to the zeros of the Hermite polynomial H_m, and we choose p_{tm} for $t \in \{1,\ldots,m\}$ such that the sequence $\{p_{tm}/\sqrt{N_S}\}_t$ is equal to the zeros of the Hermite polynomial H_m. Then the constellation is given by the following distribution:

$$\begin{aligned} r_X(x) &= r_X(\alpha_x) && (45)\\ &= r_X\left(\frac{q_{wm}+ip_{tm}}{\sqrt{2}}\right) && (46)\\ &= r_{L_m}\left(\frac{q_{wm}}{\sqrt{N_S}}\right)\, r_{L_m}\left(\frac{p_{tm}}{\sqrt{N_S}}\right) && (47)\\ &\equiv r_{Q_A}(q_{wm})\, r_{P_A}(p_{tm}), && (48)\end{aligned}$$

where $x=(w,t) \in \{1,\ldots,m\}\times\{1,\ldots,m\}$. The factor $\sqrt{N_S}$ is a scaling factor incorporated so that the mean photon number of the expected density operator for the resulting constellation is equal to the mean photon number of the thermal state $\theta(N_S)$. The phase space distribution for several discrete modulated states is give in Figure 1.

Let Q_A denote the discrete random variable with realizations $q_A \in \mathbb{R}$, taking values q_{wm} and having a probability distribution as detailed above. Let Q_B denote the random variable associated to Bob's homodyne measurement outcome of the position-quadrature operator, taking values in $\mathbb{R}$. Then, for characterizing the isometric channels $\mathcal{U}_{A\to BE}$ in $\mathcal{S}$, Alice and Bob calculate the parameters γ_{11}, γ_{12}, and γ_{22} from their data. Due to the fact that we are operating in the asymptotic regime (with no finite-size statistical effects), the following equalities hold for protocols with homodyne detection

$$\gamma_{11} = \mathbb{E}\left[(Q_A - \mathbb{E}[Q_A])^2\right], \tag{49}$$

$$\gamma_{12} = \mathbb{E}\left[(Q_A - \mathbb{E}[Q_A])(Q_B - \mathbb{E}[Q_B])\right], \tag{50}$$

$$\gamma_{22} = \mathbb{E}\left[(Q_B - \mathbb{E}[Q_B])^2\right]. \tag{51}$$

Now consider the discrete-modulation protocols with heterodyne detection. Let Q_A denote the discrete random variable with realizations $q_A \in \mathbb{R}$, taking values q_{wm} and having a probability distribution as detailed above. Let P_A denote the discrete random variable with realizations $p_A \in \mathbb{R}$, taking values p_{wm} and having a probability distribution as detailed above. Let Q_B denote the random variable associated to Bob's heterodyne measurement outcome of the position-quadrature operator, taking values in $\mathbb{R}$. Let P_B denote the random variable associated to Bob's heterodyne measurement outcome of the momentum-quadrature operator, taking values in $\mathbb{R}$. Then, in the asymptotic regime the following equalities hold for protocols with heterodyne measurement

$$\gamma_{11} = \mathbb{E}\left[(Q_A - \mathbb{E}[Q_A])^2\right] = \mathbb{E}\left[(P_A - \mathbb{E}[P_A])^2\right], \tag{52}$$

$$\begin{aligned}\gamma_{12} = \frac{1}{2}\Big(&\mathbb{E}\left[(Q_A - \mathbb{E}[Q_A])(Q_B - \mathbb{E}[Q_B])\right] + \\ &\mathbb{E}\left[(P_A - \mathbb{E}[P_A])(P_B - \mathbb{E}[P_B])\right]\Big),\end{aligned} \tag{53}$$

$$\gamma_{22} = \frac{1}{2}\left(\mathbb{E}\left[(Q_B - \mathbb{E}[Q_B])^2\right] + \mathbb{E}\left[(P_B - \mathbb{E}[P_B])^2\right]\right). \tag{54}$$

Due to the symmetry of the protocol, (53) and (54) can be simplified as

$$\gamma_{12} = \mathbb{E}\left[(Q_A - \mathbb{E}[Q_A])(Q_B - \mathbb{E}[Q_B])\right], \tag{55}$$

$$\gamma_{22} = \mathbb{E}\left[(Q_B - \mathbb{E}[Q_B])^2\right]. \tag{56}$$

As stated previously, Alice estimates γ_{11} from her preparation data, while Bob estimates γ_{22} from his measurement data. Alice calculates γ_{12} from the data that is publicly published by Bob. Then $\mathcal{S}$ is the set of isometric channels $\mathcal{U}_{A\to BE}$ that fulfill the constraints in Section III and produce the observed values of γ_{12} and γ_{22}. As a consequence, Alice and Bob deduce that the attack by Eve yields the observed values of γ_{12} and γ_{22}. In this way, they are able to restrict the possible attacks that could have been performed by Eve.

B. Estimation of parameters for a hypothetical Gaussian-modulation protocol

Now notice that the remaining Holevo information $\sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}} \chi(Y;E)_{\mathcal{E}_\theta}$ from (43) that we want to bound from above is calculated for a thermal state $\theta(N_S)$ sent over an isometric channel $\mathcal{U}_{A\to BE}$ in the set $\mathcal{S}$ and Bob performing homodyne or heterodyne detection. Therefore, we want to obtain an estimate of the parameters γ_{11}^G, γ_{12}^G, and γ_{22}^G, which are defined analogously to (49)–(51), but with the initial random variable Q_A replaced by a Gaussian random variable with mean zero and variance equal to N_S. The parameters γ_{11}^G, γ_{12}^G, and γ_{22}^G are those that would be observed in a Gaussian modulation protocol when the average channel input of Alice is a ther-

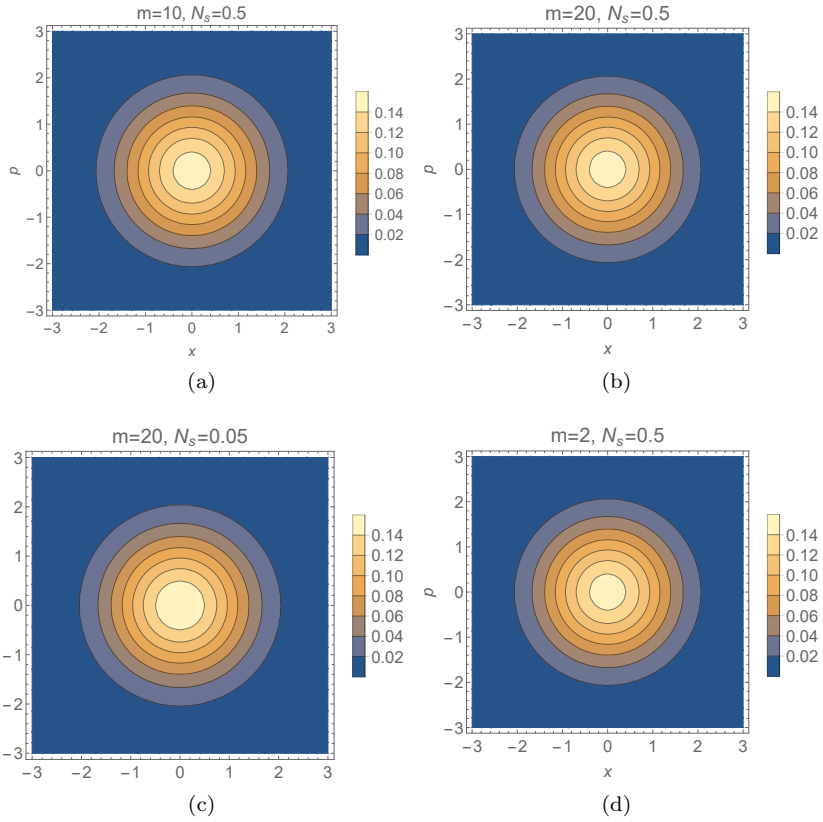

FIG. 1. In this figure, we plot the phase space distribution for the discrete modulation state $\bar{\rho}$. (a) $M = 10, N_s = .5$ (b) $M = 20, N_s = .5$ (c) $M = 20, N_s = .05$ (d) $M = 2, N_s = .5$.

mal state $\theta(N_S)$ instead of $\overline{\rho}$. A hypothetical Gaussian-modulation protocol refers to a protocol in which the average state that Alice sends is a thermal state $\theta(N_S)$ instead of $\overline{\rho}$. This protocol is not carried out by Alice and Bob experimentally, but the parameters $\gamma_{11}^G, \gamma_{12}^G, \gamma_{22}^G$ corresponding to the hypothetical Gaussian modulation protocol are inferred from the discrete-modulation protocol.

In order to bound the values of the parameters that would be obtained in a Gaussian-modulation protocol with Eve's attack taken from the set $\mathcal{S}$, we can employ the parameters that are observed in the discrete-modulation protocol. Before we do so, let us recall the definition of the χ^2 divergence of two states ρ and σ as $\chi^2(\rho,\sigma) \equiv \mathrm{Tr}\left[(\rho\sigma^{-1/2})^2\right] - 1$ [63]. Then we have the following proposition:

Proposition 1 *Let* $\overline{\rho} = \sum_x r_X(x) |\alpha_x\rangle\langle\alpha_x|$, *where*

$$\alpha_x = \frac{q_A + ip_A}{\sqrt{2}}, \tag{57}$$

$$r_X(x) = r_{Q_A}(q_A)\, r_{P_A}(p_A), \tag{58}$$

$$\theta_{N_S} = \int dx\, r_X^G(x) |\alpha_x\rangle\langle\alpha_x|, \tag{59}$$

and $r^G(x)$ *is the P-function of a thermal state with mean photon number* N_S. *If* $\sqrt{\chi^2(\overline{\rho}, \theta(N_S))} \leq \varepsilon^2$, *and Eve's attacks fulfill the constraints in Section III, then*

$$\gamma_{11} = \gamma_{11}^G, \tag{60}$$

$$|\gamma_{22} - \gamma_{22}^G| \leq \varepsilon_1, \tag{61}$$

$$|\gamma_{12} - \gamma_{12}^G| \leq \varepsilon_2, \tag{62}$$

where

$$\varepsilon_1 \equiv \varepsilon \cdot (1 + c_1) \cdot \sqrt{\mathbb{E}\left[(Q_B - \mathbb{E}[Q_B])^4\right]}, \tag{63}$$

for some constant $c_1 > 0$ *and*

$$\begin{aligned}\varepsilon_2 \equiv & \sum_{k=0}^{2m-2} \sum_{l=2m}^{K} \mu_{kl} \left|\eta^G(q_A, k+1)\left(\eta^G(p_A, l) - \eta(p_A, l)\right)\right| \\ & + \sum_{k=2m-1}^{K} \sum_{l=0}^{2m-1} \mu_{kl} \left|\eta^G(p_A, l)\left(\eta^G(q_A, k+1) - \eta(q_A, k+1)\right)\right| \\ & + \sum_{k=2m-1, l=2m}^{K} \mu_{kl} \left|\eta^G(p_A, l)\eta^G(q_A, k+1) - \right. \\ & \left. \eta(p_A, l)\eta(q_A, k+1)\right|, \end{aligned} \tag{64}$$

where μ_{kl} *is an arbitrary function for* $k \leq 2m-2$, $l \leq 2m-1$ *and is equal to* $\exp(-a(k+l))$ *otherwise. We also define the following quantities*

$$\eta^G(q_A, k) \equiv \mathbb{E}_{r_{Q_A}^G}[Q_A^k], \tag{65}$$

$$\eta(q_A,k) \equiv \mathbb{E}_{r_{Q_A}}[Q_A^k], \tag{66}$$
$$\eta^G(p_A,k) \equiv \mathbb{E}_{r^G_{P_A}}[P_A^k], \tag{67}$$
$$\eta(p_A,k) \equiv \mathbb{E}_{r_{P_A}}[P_A^k]. \tag{68}$$

Our proof of (61) relies mainly on the properties of trace distance, invoking the Cauchy–Schwarz inequality and the assumption that the fourth moment of the channel output is bounded. Our proof of (62) relies mainly on the properties of Gauss-Hermite distribution, and on the last assumption in Section III. For details, please refer to Appendix A. By invoking Proposition 1, we conclude that $\gamma^G_{22} \in [\gamma_{22}-\varepsilon_1, \gamma_{22}+\varepsilon_1]$, and $\gamma^G_{12} \in [\gamma_{12}-\varepsilon_2, \gamma_{12}+\varepsilon_2]$, where ε_1 and ε_2 are defined above.

Now, consider the following scenario corresponding to an entanglement-based (EB) QKD protocol: Alice prepares a two-mode squeezed vacuum state $\psi(\bar{n})_{RA} = |\psi(\bar{n})\rangle\langle\psi(\bar{n})|_{RA}$ where

$$|\psi(\bar{n})\rangle_{RA} \equiv \frac{1}{\sqrt{\bar{n}+1}} \sum_{n=0}^{\infty} \sqrt{\left(\frac{\bar{n}}{\bar{n}+1}\right)^n} |n\rangle_R |n\rangle_A, \tag{69}$$

with $\bar{n} \geq 0$. She applies a phase $e^{-i\hat{n}\pi k/2}$ to her channel input mode A, with $k \in \{0,1,2,3\}$ selected uniformly at random, and she sends the system A to Bob over an isometric channel $\mathcal{U}^{\mathcal{N}}_{A\to BE}$ selected from the set $\mathcal{S}$. She also communicates k to Bob over an authenticated public classical channel. Bob then applies the inverse phase $e^{-i\hat{n}\pi k/2}$. Both Alice and Bob then discard the value of k. Let ρ_{RB} denote the state shared by Alice and Bob at the end, so that the reduced channel $\mathcal{N}_{A\to B}$ has been phase symmetrized due to the protocol above and with $\overline{\mathcal{N}}_{A\to B}$ defined as in (2):

$$\rho_{RB} \equiv \overline{\mathcal{N}}_{A\to B}(\psi(\bar{n})_{RA}). \tag{70}$$

Due to the symmetries of the two-mode squeezed vacuum state $\psi(\bar{n})_{RA}$ as well as those of the phase-symmetrized channel $\overline{\mathcal{N}}_{A\to B}$, it follows that the covariance matrix of the state ρ_{RB} has the following form:

$$\begin{bmatrix} \gamma^{\mathrm{EB}}_{11}\mathbb{I}_2 & \gamma^{\mathrm{EB}}_{12}R(\theta) \\ \gamma^{\mathrm{EB}}_{12}R(\theta) & \gamma^{\mathrm{EB}}_{22}\mathbb{I}_2 \end{bmatrix}, \tag{71}$$

where $\gamma^{\mathrm{EB}}_{11}, \gamma^{\mathrm{EB}}_{12}, \gamma^{\mathrm{EB}}_{22} \in \mathbb{R}$ such that the matrix above is a legitimate quantum covariance matrix [64], the matrix $\mathbb{I}_2$ is the 2×2 identity matrix, and

$$R(\theta) \equiv \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix}, \tag{72}$$

is a rotation matrix. See Appendix B for a proof of this claim. In what follows, we assume that $\theta = 0$, due to the fact that doing so simplifies the protocol, as well as reduces the number of parameters that need to be estimated, and it furthermore does not lead to an increase in Eve's Holevo information, as discussed in [25]. Alice then performs a heterodyne measurement on mode R and Bob performs a homodyne or a heterodyne measurement on mode B. As mentioned above, this is the entanglement-based (EB) version of the Gaussian-modulated prepare-measure (PM) protocol with the attacks by Eve constrained to the set $\mathcal{S}$.

Now, we want to deduce the parameters $\gamma^{\mathrm{EB}}_{11}, \gamma^{\mathrm{EB}}_{12}, \gamma^{\mathrm{EB}}_{22}$ observed in the EB protocol from the parameters $\gamma^G_{11}, \gamma^G_{12}, \gamma^G_{22}$ observed in the PM version of the Gaussian modulation protocol. As is common in the CV-QKD literature, we consider the EB protocol because it is helpful in analyzing the Holevo information $\chi(Y;E)$ that results in the prepare-measure (PM) protocol. The "PM to EB" mapping of the parameters is well known in the literature [65] and is given as follows for protocol where Bob performs homodyne detection:

$$\gamma^{\mathrm{EB}}_{11} = \gamma^G_{11} + 1 = \gamma_{11} + 1, \tag{73}$$
$$\gamma^{\mathrm{EB}}_{22} = \gamma^G_{22} \in [\gamma_{22}-\varepsilon_1, \gamma_{22}+\varepsilon_1], \tag{74}$$
$$\gamma^{\mathrm{EB}}_{12} = \sqrt{\frac{\gamma_{11}+2}{\gamma_{11}}}\gamma^G_{12} \in \left[\sqrt{\frac{\gamma_{11}+2}{\gamma_{11}}}(\gamma_{12}-\varepsilon_2), \sqrt{\frac{\gamma_{11}+2}{\gamma_{11}}}(\gamma_{12}+\varepsilon_2)\right]. \tag{75}$$

For protocols where Bob performs heterodyne detection the "PM to EB" mapping of the parameters is given by

$$\gamma^{\mathrm{EB}}_{11} = \gamma^G_{11} + 1 = \gamma_{11} + 1, \tag{76}$$
$$\gamma^{\mathrm{EB}}_{22} = 2\gamma^G_{22} - 1 \in [2\gamma_{22} - 1 - \varepsilon_1, 2\gamma_{22} - 1 + \varepsilon_1], \tag{77}$$
$$\gamma^{\mathrm{EB}}_{12} = \sqrt{\frac{2(\gamma_{11}+2)}{\gamma_{11}}}\gamma^G_{12} \in \left[\sqrt{\frac{2(\gamma_{11}+2)}{\gamma_{11}}}(\gamma_{12}-\varepsilon_2), \sqrt{\frac{2(\gamma_{11}+2)}{(\gamma_{11}}}(\gamma_{12}+\varepsilon_2)\right]. \tag{78}$$

Let Σ denote the set of quantum states ρ_{RB} that have covariance matrix of the following form:

$$\begin{bmatrix} \gamma^{\mathrm{EB}}_{11}\mathbb{I}_2 & \gamma^{\mathrm{EB}}_{12}\sigma_Z \\ \gamma^{\mathrm{EB}}_{12}\sigma_Z & \gamma^{\mathrm{EB}}_{22}\mathbb{I}_2 \end{bmatrix}. \tag{79}$$

C. Upper bound on Eve's Holevo information

By applying purification techniques of quantum information theory, the following equality holds

$$\chi(Y;E)_{\mathcal{E}_\theta} = H(RB)_\rho - H(R|Y)_{\{p(y),\rho^y\}_y}, \tag{80}$$

for ρ_{RB} the state in (70) and $\{p(y),\rho^y_R\}_y$ the ensemble resulting from Bob performing a position-quadrature homodyne detection, or a heterodyne detection on the state ρ_{RB}. As a consequence, the task of obtaining an upper bound on $\sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}} \chi(Y;E)_{\mathcal{E}_\theta}$ can be accomplished by obtaining an upper bound on $\sup_{\rho_{RB}\in\Sigma}\left(H(RB)_\rho - H(R|Y)_{\{p(y),\rho^y\}_y}\right)$.

We then invoke the extremality of Gaussian states [57, 59], from which we infer that the Holevo information is optimized by a Gaussian state ρ_{RB}^{G} having the same covariance matrix as ρ_{RB}. Therefore, we obtain the following:

$$\sup_{\rho_{RB}\in\Sigma}\left(H(RB)_{\rho}-H(R|Y)_{\{p(y),\rho^{y}\}}\right) = \sup_{\rho_{RB}^{G}\in\Sigma}\left(H(RB)_{\rho^{G}}-H(R|Y)_{\{p^{G}(y),\rho^{y,G}\}}\right), \quad (81)$$

where $\{p^{G}(y),\rho_{R}^{y,G}\}$ is the ensemble obtained if Bob performs a homodyne/heterodyne measurement on mode B of ρ_{RB}^{G}.

Then, Eve's Holevo information can be calculated as follows:

$$H(RB)_{\rho^{G}}-H(R|Y)_{\{p^{G}(y),\rho^{y,G}\}} = g(\nu_1)+g(\nu_2)-g(\nu_3), \quad (82)$$

where the function $g(\cdot)$ is defined in (40), ν_1 and ν_2 are the symplectic eigenvalues of the covariance matrix in (79). For protocols where Bob performs homodyne detection, $\nu_3=\gamma_{11}^{\mathrm{EB}}\left(\gamma_{11}-\frac{(\gamma_{12}^{\mathrm{EB}})^2}{\gamma_{22}^{\mathrm{EB}}+1}\right)$. For protocols where Bob performs heterodyne detection, $\nu_3=\gamma_{11}^{\mathrm{EB}}-\frac{(\gamma_{22}^{\mathrm{EB}})^2}{\gamma_{12}^{\mathrm{EB}}+1}$. Numerical checks, similar to those performed and stated in [25], reveal that the Holevo information is a monotonically decreasing function of $\gamma_{12}^{\mathrm{EB}}$, and a monotonically increasing function of $\gamma_{11}^{\mathrm{EB}}$ and $\gamma_{22}^{\mathrm{EB}}$. Intuitively, the correlations between Alice and Bob are quantified by $\gamma_{12}^{\mathrm{EB}}$, so that increasing this parameter decreases Eve's Holevo information.

Therefore, we conclude that the Holevo information for protocols where Bob performs homodyne detection is no larger than that achieved by a Gaussian state ρ_{RB} that has a covariance matrix as follows:

$$\begin{bmatrix}(\gamma_{11}+1)\mathbb{I} & \sqrt{\frac{\gamma_{11}+2}{\gamma_{11}}}(\gamma_{12}-\varepsilon_2)\sigma_Z\\ \sqrt{\frac{\gamma_{11}+2}{\gamma_{11}}}(\gamma_{12}-\varepsilon_2)\sigma_Z & (\gamma_{22}+\varepsilon_1)\mathbb{I}\end{bmatrix}. \quad (83)$$

The Holevo information for protocols where Bob performs heterodyne detection is no larger than that achieved by a Gaussian state ρ_{RB} that has a covariance matrix as follows:

$$\begin{bmatrix}(\gamma_{11}+1)\mathbb{I} & \sqrt{\frac{2(\gamma_{11}+2)}{\gamma_{11}}}(\gamma_{12}-\varepsilon_2)\sigma_Z\\ \sqrt{\frac{2(\gamma_{11}+2)}{\gamma_{11}}}(\gamma_{12}-\varepsilon_2)\sigma_Z & (2\gamma_{22}-1+\varepsilon_1)\mathbb{I}\end{bmatrix}. \quad (84)$$

With this, we conclude our goal of obtaining an upper bound on the remaining term $\sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}}\chi(Y;E)_{\mathcal{E}_\theta}$.

In Appendix C, we give an alternative method to upper bound the Holevo information $\sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}}\chi(Y;E)_{\mathcal{E}_\rho}$ in (42). The proposed method does not depend on the parameters c_1, K and a; however, it seems to be numerically intensive.

VI. NUMERICAL RESULTS FOR A LOSSY THERMAL BOSONIC CHANNEL

We now proceed with calculating the various terms in (43) for a Gauss-Hermite constellation of size m^2 and for a lossy thermal bosonic channel of transmissivity $\eta\in[0,1]$ and $N_B\geq 0$. This allows for determining the performance of the discrete-modulation CV-QKD protocol when the underlying channel is a lossy thermal channels (however, keep in mind that Alice and Bob are not aware of this when executing the protocol).

The first term that we need to calculate is the Shannon mutual information $I(X;Y)$. Here, X is a random variable that encodes the choice of coherent state, and Y is the random variable that is associated with the measurement result. For discrete-modulation protocols with homodyne detection and the underlying channel as the pure-loss channel, we use the following approach: The Wigner function associated with the coherent state $|\alpha_x\rangle$ subjected to a pure-loss channel with transmissivity η is given as

$$W_{y,p}^{\alpha_x}=\frac{1}{\pi}\exp\Big\{-|z-\sqrt{\eta}\alpha_x|^2\Big\}, \quad (85)$$

where $z=q_B+ip_B$, with the real part q_B corresponding to the position-quadrature phase-space variable, and the imaginary part p_B corresponding to the momentum-quadrature phase-space variable. Bob performs homodyne detection with respect to the q_B quadrature, which provides the raw data for key generation. Then the various probability distributions are given as

$$r_X(x)=Q_{N_S,m}(\alpha_x), \quad (86)$$

$$r_{Y|X}(q_B|x)=\int_{-\infty}^{\infty}dp_B\ W_{q_B,p_B}^{\alpha_x}, \quad (87)$$

$$r_Y(q_B)=\sum_x r_X(x)r_{Y|X}(q_B|x). \quad (88)$$

With this information in hand, it is easy to calculate $I(X;Y)=H(Y)_r-H(Y|X)_r$. Now, let us calculate $I(X;Y)$ for the discrete modulation protocols with heterodyne detection. Alice sends a coherent state characterized by $|\alpha_x\rangle$ through a thermal channel characterized by η and N_B. After the transmission, Bob has a displaced thermal state with the mean vector $\bar{r}_{\mathrm{final}}$ and covariance matrix σ_{final}. These can be written as

$$\bar{r}_{\mathrm{final}}=\sqrt{\eta}\,\bar{r}_{\mathrm{coherent}}=\sqrt{\eta}\left[\sqrt{2}q_{wm},\sqrt{2}p_{tm}\right]^T, \quad (89)$$

$$\sigma_{\mathrm{final}}=\eta\,\sigma_{\mathrm{coherent}}+(1-\eta)(2N_B+1)\mathbb{I}_2 = \eta\,\mathbb{I}_2+(1-\eta)(2N_B+1)\mathbb{I}_2, \quad (90)$$

where $\bar{r}_{\mathrm{coherent}}$ is the mean vector and $\sigma_{\mathrm{coherent}}$ is the covariance matrix of the coherent state $|\alpha_x\rangle=\left|\frac{q_{wm}+ip_{tm}}{\sqrt{2}}\right\rangle$. Then the various probability distributions are given as

$$r_{Y|X}(q_b,p_b|q_{wm},p_{tm})=\frac{\exp\left[-\frac{(q_b-\sqrt{2}q_{wm})^2-(p_b-\sqrt{2}p_{tm})^2}{2(1-N_B(1-\eta))}\right]}{\pi\sqrt{\mathrm{Det}\left[2(1-N_B(1-\eta))\mathbb{I}_2\right]}} \quad (91)$$

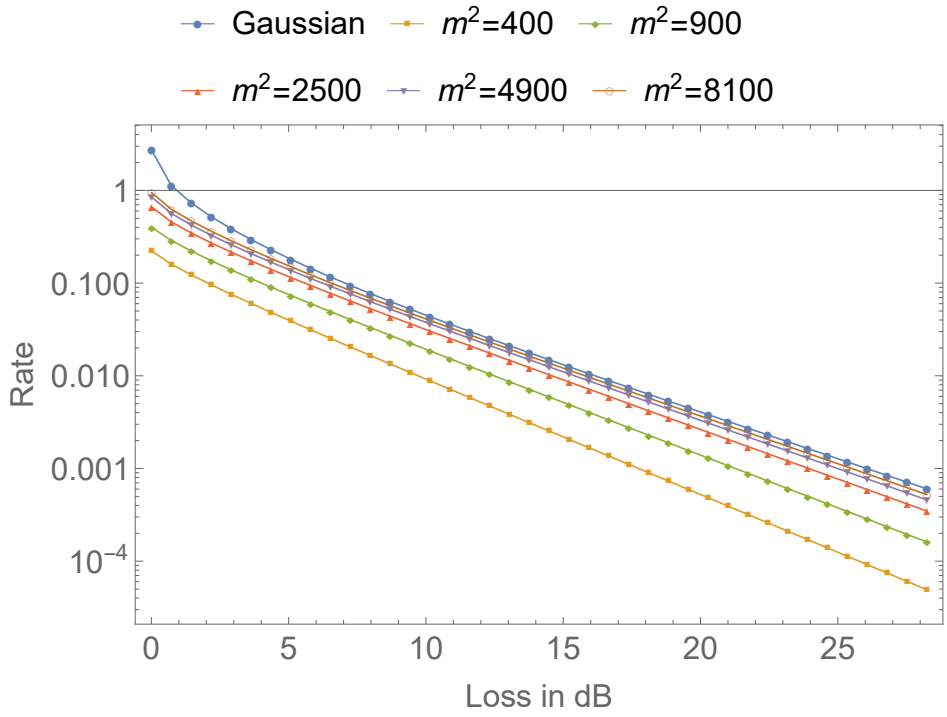

FIG. 2. In this figure, we plot the lower bounds on the key rates for various constellation size m^2 of the discrete-modulation protocol considered in Section II with the underlying channel as a lossy bosonic channel

$$r_Y(q_b,p_b)=\sum_{q_{wm},p_{tm}} r_X(q_{wm},p_{tm})r_{Y|X}(q_b,p_b|q_{wm},p_{tm}). \tag{92}$$

With this information, we can easily calculate $I(X;Y)$. Numerically, we find that $I(X;Y)$ calculated from the above method is approximately equal to the $I(X;Y)$ that we obtain from a Gaussian modulation protocol with the underlying channel as thermal channel. We invoke this approximation in the numerics. This approximation has been proven rigorously in [45].

The second term that we need to calculate is the Holevo information $\sup_{\mathcal{U}_{A\to BE}\in\mathcal{S}}\chi(Y;E)_{\mathcal{E}_\theta}$ for a key-generation protocol that uses Gaussian modulation of coherent states and homodyne/heterodyne detection. To this end, we need to calculate the parameters γ_{11}, γ_{22}, and γ_{12} for the discrete-modulation protocol in order to obtain the covariance matrix in (83) or in (84). These can be calculated numerically. However, note that $\theta(N_S)$ and $\overline{\rho}$ have the same covariance matrix due to the second moment of the Gauss-Hermite approximation and Gaussian distribution being the same. Since we are considering the underlying channel as a lossy thermal bosonic channel, we can calculate the parameters γ_{22} and γ_{12} using the analytical formulas given in Section 7 of [65]. From the values of γ_{12} and γ_{22} we now have to estimate the parameters γ_{12}^G and γ_{22}^G. To this end, we apply Proposition 1. When applying Proposition 1, it is necessary to make a choice for the parameters c_1, a and K. In our example considered here, we take the conservative choices $c_1=100$, $K=10^4$, and $a=5$.

Next, we have to calculate the third term, which is the error introduced in the Holevo information $\chi(Y;E)$ and denoted by $f(\varepsilon,N_S')$ in (43). To this end, we first calculate the approximation error ε defined in (21). Following [45], we use the χ^2-distance, defined as $\chi^2(\rho,\sigma)\equiv \mathrm{Tr}[(\rho\sigma^{-1/2})^2]-1$, and we employ the bound $\|\rho-\sigma\|_1^2\leq\chi^2(\rho,\sigma)$, which follows from Lemma 5 of [63] with $k=1/2$.

Let us denote an additive white Gaussian noise channel with signal to noise ratio s by W_s. The action of W_s is defined as $W_s(Z)=\sqrt{s}Z+G$, where G is a normally distributed random variable with unit variance. Then, for $Z\sim\mathcal{N}(0,1)$ with distribution P_Z, a random variable Z_m' with distribution P_{Z_m} as given in (44), $Y=W_s(Z)$, and $Y_m'=W_s(Z_m')$, the χ^2 distance is given as

$$\chi^2\left(P_{Y_m'},P_Y\right)=2\kappa^2\sum_{k\geq m}\left(\frac{s}{1+s}\right)^{2k} \tag{93}$$

$$=2\kappa^2\frac{(1+s)^2}{1+2s}\left(\frac{s}{1+s}\right)^{2m}, \tag{94}$$

with $2\kappa^2\approx 2.36$ [44].

Let

$$\overline{\rho}_m=\sum_{x=1}^{m^2}Q_{N_S,m}(\alpha_x)\,|\alpha_x\rangle\langle\alpha_x|\,, \tag{95}$$

and θ_{N_S} be a thermal state of mean photon number N_S.

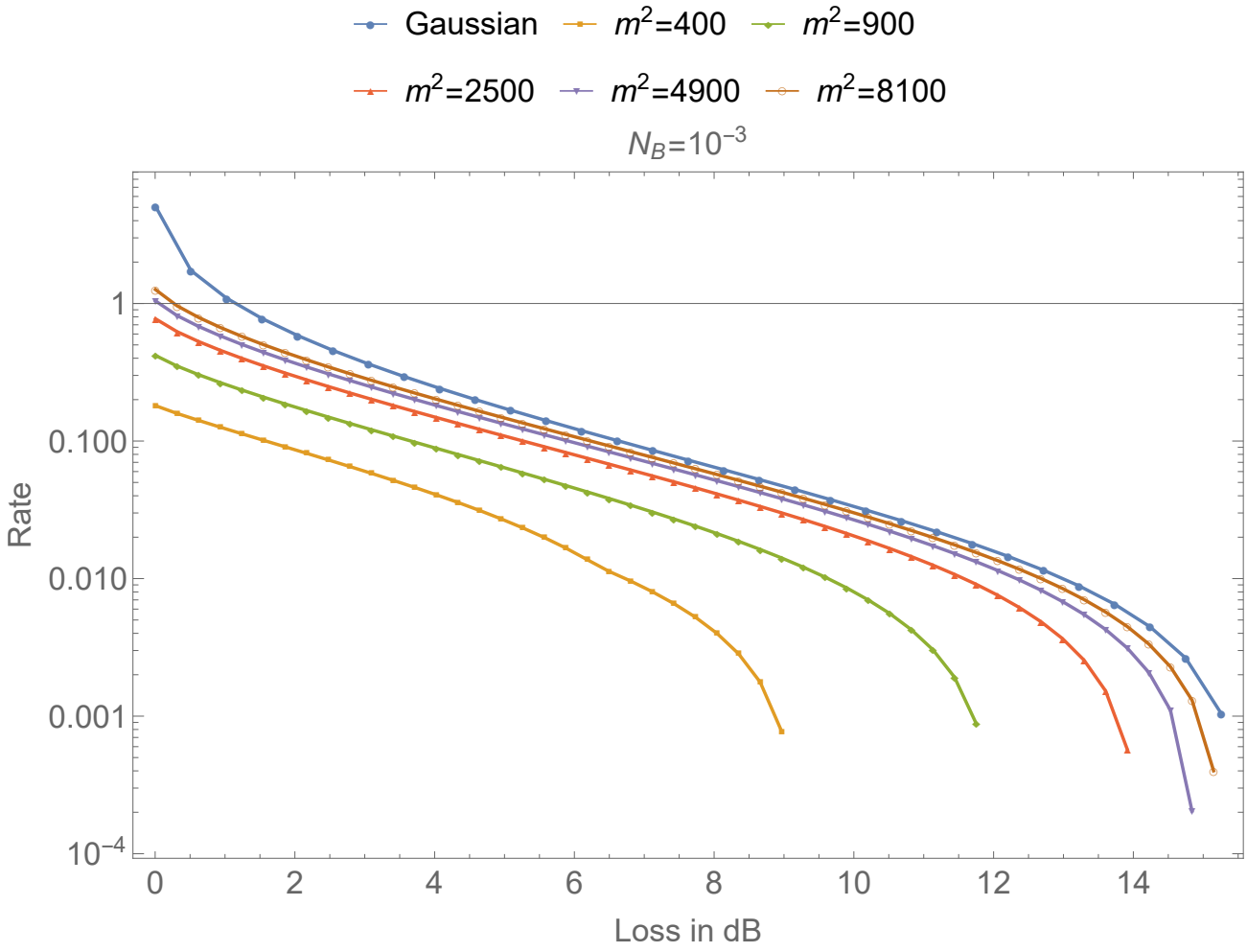

FIG. 3. In this figure, we plot the lower bounds on the key rate for various constellation size m^2 of the discrete-modulation protocol considered in Section II with the underlying channel as a lossy thermal bosonic channel with thermal noise $N_B = 10^{-3}$.

Then

$$\chi^2(\overline{\rho}_m, \theta_{N_S}) = \left(1 + \chi^2(P_{Y_m}, P_Y)\right)^2 - 1, \tag{96}$$
$$= (1+\tau)^2 - 1 \tag{97}$$
$$= \tau(2+\tau), \tag{98}$$

with $s = N_S / \left(\sqrt{N_S(N_S+1)} - N_S\right)$ [45] and

$$\tau \equiv 2\kappa^2 \left(1 + N_S\right) \left(\frac{N_S}{\sqrt{N_S(1+N_S)}}\right)^{2m}. \tag{99}$$

Combining (93) and (96), we obtain the following expression for the approximation error:

$$\frac{1}{2}\|\overline{\rho}_m - \theta_{N_S}\|_1 \leq \varepsilon = \frac{1}{2}\sqrt{\tau(2+\tau)}. \tag{100}$$

We can then invoke [46, Proposition 27], which utilizes some techniques from [53], to obtain

$$f(\varepsilon, N_S) = \varepsilon\left(2t + r_\varepsilon(t)\right) g(P/\varepsilon t) + 2g(\varepsilon r_\varepsilon(t)) + 2h(\varepsilon t), \tag{101}$$

for any $t \in (0, \frac{1}{2\varepsilon}]$, where

$$r_\varepsilon(t) = (1 + t/2)/(1 - \varepsilon t), \tag{102}$$
$$P = 10^7, \tag{103}$$
$$g(N) = (N+1)\log_2(N+1) - N\log_2(N), \tag{104}$$
$$h(x) = -x\log_2(x) - (1-x)\log_2(1-x). \tag{105}$$

In the above, we have set $P = 10^7$, which is an extremely conservative choice to employ with respect to the fourth assumption on Eve's attack discussed in Section III. We have also supposed that Eve's system is a harmonic oscillator. Even though the mean photon number of the average input state in all example cases that we consider in what follows is many orders of magnitude smaller than $P = 10^7$ and the actual physical channel being employed is a pure-loss channel, we can still suppose that the mean energy of the eavesdropper's states is extremely large (way beyond what an eavesdropper

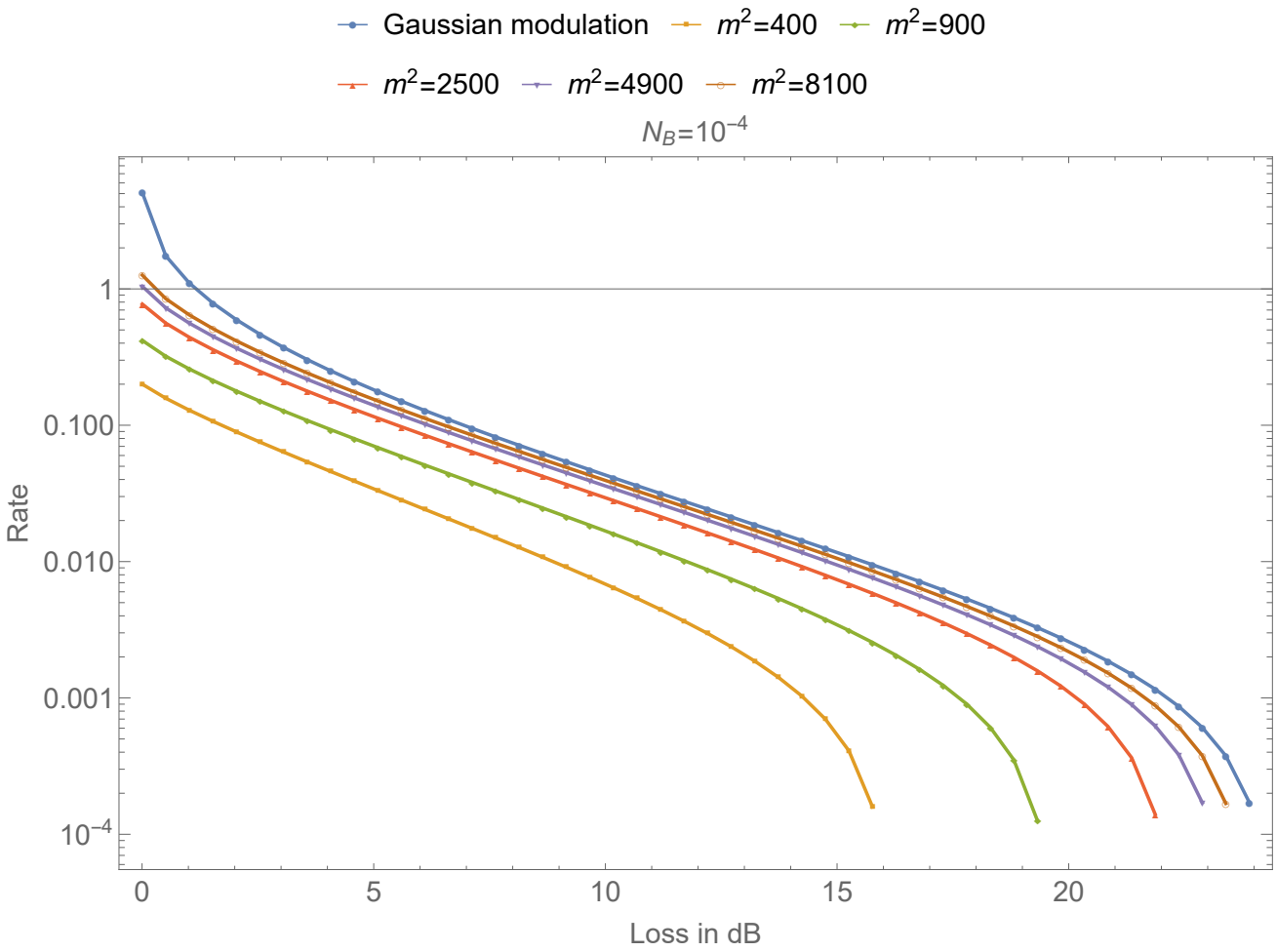

FIG. 4. In this figure, we plot the lower bounds on the key rate for various constellation size m^2 of the discrete-modulation protocol considered in Section II with the underlying channel as a lossy thermal bosonic channel $N_B = 10^{-4}$.

might reasonably employ in an attack) and we find that the performance of the discrete-modulation protocols approaches that of the Gaussian-modulation protocol relatively quickly as the constellation size m^2 increases. One could choose an even more conservative value for P, higher than what we have taken. However, in our numerics, we have found the same qualitative behavior: that the performance of the discrete-modulation protocol rapidly approaches that of the Gaussian-modulation protocol as the constellation size m^2 increases.

With all these ingredients in hand, we can now numerically evaluate (43) to obtain a lower bound on the secret-key rate for a lossy thermal bosonic channel with transmissivity η and thermal noise as N_B. We take the reconciliation efficiency $\beta = 0.95$. Note that the key rates obtained from (43) have a dependence on the mean photon number N_S of the input state. Thus, to obtain tight lower bounds on the secret-key rate, we also optimize over N_S.

In Figure 2, we present the achievable key rates obtained from discrete-modulation protocol with homodyne detection if the underlying channel is a pure-loss channel. In Figures 3, and 4, we present the achievable key rates from discrete-modulation protocol with heterodyne detection if the underlying channel is a thermal channel. We plot lower bounds for various values of m^2 and compare the obtained lower bounds with the Gaussian-modulation protocol. It is clear that the secure key rate of the discrete-modulation protocol increases as the constellation size m^2 increases.

As explained before, to obtain the lower bound on the rates for pure-loss channel and thermal channel, we optimize over the mean photon number N_S. For the Gaussian-modulation protocol, we find that the optimal variance for secret-key rates decreases with the increase in loss. Now, the main idea behind the technique presented in this paper is to discretize the Gaussian probability distribution by a finite constellation of size m^2 and calculate the error introduced due to this approximation. We find that as the variance of the Gaussian modulation increases, the number of constellation points required to approximate the distribution to an ε error

increases. Therefore, for low losses, this technique requires a large number m^2 of constellation points to closely match the secret key-rates obtained with Gaussian modulation.

A consequence of the aforementioned reasoning is that, with our approach, the lower bound on the secret-key rate does not tend to $\log m^2$ in the limit as $\eta \to 1$. Certainly, in this limit, the Holevo information with Eve tends to zero, and the key rate is then given as $K \geq I(X;Y) - f(\varepsilon, N'_S)$. We numerically observe that the Shannon mutual information of Alice and Bob saturates towards $\log m^2$ with the increase in variance; however, the approximation error $f(\varepsilon, N'_S)$ increases with the increase in variance. Due to this trade-off, our technique does not achieve the ideal rate of $\log m^2$ rate in the low-loss and low-noise limit.

It is possible (and likely) that our rate lower bounds can be improved by other constellation choices or other proof techniques. However, even with our proof, requiring a pair of electro-optic (phase and amplitude) modulators to generate a 90×90 size constellation size is much more practical and less demanding compared to asking that we modulate a pulse with a complex amplitude to an extremely high floating point accuracy, which a Gaussian modulation would need.

We should also point out that dark counts in detectors can be modeled as thermal noise for lossy thermal bosonic channels [66]. Thus, our numerics are also applicable to protocols with imperfect detectors modeled in this way.

We note here that we have included in the arXiv posting of this paper the Mathematica files used to perform the numerical calculation of the key rates and to generate the figures.

VII. CONCLUSION

In this paper, we have addressed an open problem in continuous-variable quantum key distribution (CV-QKD), by establishing a security proof for discrete-modulation protocols. Even though many experiments have been performed on discrete-modulation CV-QKD with multiple constellation points (see, e.g., [67–69]), no security proofs have been available for them, and the expected key-rate calculations previously reported based on measured homodyne statistics have been based on assuming Gaussian attacks, which are not known to be optimal for discrete-modulation CV-QKD. We have introduced a discrete-modulation protocol and then obtained rigorous lower bounds on the secret-key rates, secure against physically reasonable collective attacks in the asymptotic key-length regime. The approach that we have used works well in the high-loss regime, with the secure key rates being close to the secure key rates achievable with a Gaussian-modulation protocol. Another prominent feature of our approach is that with the increase in the size m^2 of the constellation, the lower bound on the secret-key rate approaches the key rate for the Gaussian-modulation protocol. This result demonstrates that we need not consider the full continuum of the Gaussian distribution in order to obtain key rates achievable with a Gaussian modulation, and we do not need to rely on Gaussian modulation for security proofs of discrete-modulation CV-QKD protocols.

Going forward from here, it is a pressing open question to determine security proofs for discrete-modulation CV-QKD protocols in the non-asymptotic, or finite key-length, regime. It would also be ideal to improve the bound from Proposition 1 to reduce or eliminate its dependence on the parameters c_1, a, and K. In this context, it might be possible to utilize the results presented in Appendix C, but as mentioned previously, this approach is numerically intensive.

ACKNOWLEDGMENTS

We are grateful to Hari Krovi for discussions about CV-QKD with discrete modulation. We are especially grateful to Anthony Leverrier for his critical reading of the initial version of our paper, for pointing out the need for more details of the channel estimation procedure, and for the idea behind Eq. (162). We thank Jeffrey H. Shapiro, Xiang-Bin Wang, and Cosmo Lupo for helpful feedback on our manuscript. This work was supported by the Office of Naval Research program Communications and Networking with Quantum Operationally-Secure Technology for Maritime Deployment (CONQUEST): Raytheon BBN Technologies prime contract number N00014-16-C2069, under subcontracts to Louisiana State University and University of Arizona.

[1] Charles H. Bennett and Gilles Brassard, "Quantum cryptography: Public key distribution and coin tossing," International Conference on Computers, Systems & Signal Processing, Bangalore, India, December 9-12, 1984 , 175–179 (1984).

[2] Artur K. Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters **67**, 661–663 (1991).

[3] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lütkenhaus, and Momtchil Peev, "The security of practical quantum key distribution," Reviews of Modern Physics **81**, 1301–1350 (2009), arXiv:0802.4155.

[4] Won-Young Hwang, "Quantum key distribution with high loss: Toward global secure communication," Physical Review Letters **91**, 057901 (2003), arXiv:quant-ph/0211153.

[5] Xiang-Bin Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Physical Review Letters **94**, 230503 (2005), arXiv:quant-ph/0410075.

[6] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, "Decoy state quantum key distribution," Physical Review Letters **94**, 230504 (2005), arXiv:quant-ph/0411004.

[7] Liang Jiang, Jacob M. Taylor, Kae Nemoto, William J. Munro, Rodney Van Meter, and M. D. Lukin, "Quantum repeater with encoding," Physical Review A **79**, 032325 (2009), arXiv:0809.3629.

[8] Sreraman Muralidharan, Linshu Li, Jungsang Kim, Norbert Lütkenhaus, Mikhail D. Lukin, and Liang Jiang, "Optimal architectures for long distance quantum communication," Scientific Reports **6**, 20463 (2016), arXiv:1509.08435.

[9] Saikat Guha, Hari Krovi, Christopher A. Fuchs, Zachary Dutton, Joshua A. Slater, Christoph Simon, and Wolfgang Tittel, "Rate-loss analysis of an efficient quantum repeater architecture," Physical Review A **92**, 022357 (2015), arXiv:1404.7183.

[10] Mihir Pant, Hari Krovi, Dirk Englund, and Saikat Guha, "Rate-distance tradeoff and resource costs for all-optical quantum repeaters," Physical Review A **95**, 012304 (2017), arXiv:1603.01353.

[11] Sreraman Muralidharan, Chang-Ling Zou, Linshu Li, and Liang Jiang, "One-way quantum repeaters with quantum Reed-Solomon codes," Physical Review A **97**, 052316 (2018), arXiv:1801.06706.

[12] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," Nature Communications **5**, 5235 (2014), arXiv:1504.06390.

[13] S. Pirandola *et al.*, Nat. Comm. **8**, 15043 (2017).

[14] Mark M. Wilde, Marco Tomamichel, and Mario Berta, "Converse bounds for private communication over quantum channels," IEEE Transactions on Information Theory **63**, 1792–1817 (2017), arXiv:1602.08898.

[15] Josephine Dias and Timothy C. Ralph, "Quantum repeaters using continuous-variable teleportation," Physical Review A **95**, 022312 (2017), arXiv:1611.02794.

[16] Fabian Furrer and William J. Munro, "Repeaters for continuous-variable quantum communication," Physical Review A **98**, 032335 (2018), arXiv:1611.02795.

[17] Kaushik P. Seshadreesan, Hari Krovi, and Saikat Guha, "A continuous-variable quantum repeater with quantum scissors," Physical Review Research **2**, 013310 (2020), arXiv:1811.12393.

[18] Quyen Dinh Xuan, Zheshen Zhang, and Paul L. Voss, "A 24 km fiber-based discretely signaled continuous variable quantum key distribution system," Optics Express **17**, 24244 (2009), arXiv:0910.1042.

[19] Xu-Yang Wang, Zeng-Liang Bai, Shao-Feng Wang, Yong-Min Li, and Kun-Chi Peng, "Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise," Chinese Physics Letters **30**, 010305 (2013).

[20] Duan Huang, Dakai Lin, Chao Wang, Weiqi Liu, Shuanghong Fang, Jinye Peng, Peng Huang, and Guihua Zeng, "Continuous-variable quantum key distribution with 1 Mbps secure key rate," Optics Express **23**, 17511 (2015).

[21] Xuyang Wang, Siyou Guo, Pu Wang, Wenyuan Liu, and Yongmin Li, "Realistic rate–distance limit of continuous-variable quantum key distribution," Optics Express **27**, 13372 (2019).

[22] Hui Liu, Wenyuan Wang, Kejin Wei, Xiao-Tian Fang, Li Li, Nai-Le Liu, Hao Liang, Si-Jie Zhang, Weijun Zhang, Hao Li, Lixing You, Zhen Wang, Hoi-Kwong Lo, Teng-Yun Chen, Feihu Xu, and Jian-Wei Pan, "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels," Phys. Rev. Lett. **122**, 160501 (2019), arXiv:1808.08584.

[23] Nathan Walk, Sara Hosseini, Jiao Geng, Oliver Thearle, Jing Yan Haw, Seiji Armstrong, Syed M. Assad, Jiri Janousek, Timothy C. Ralph, Thomas Symul, Howard M. Wiseman, and Ping Koy Lam, "Experimental demonstration of gaussian protocols for one-sided device-independent quantum key distribution," Optica **3**, 634 (2016), arXiv:1405.6593.

[24] Frédéric Grosshans and Philippe Grangier, "Continuous variable quantum cryptography using coherent states," Physical Review Letters **88**, 057902 (2002), arXiv:quant-ph/0109084.

[25] Anthony Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," Physical Review Letters **114**, 070501 (2015), arXiv:1408.5689.

[26] Nicolas J. Cerf, M. Lévy, and Gilles Van Assche, "Quantum distribution of Gaussian keys using squeezed states," Physical Review A **63**, 052311 (2001), arXiv:quant-ph/0008058.

[27] F. Furrer, T. Franz, Mario Berta, Anthony Leverrier, Volkher B. Scholz, Marco Tomamichel, and Reinhard F. Werner, "Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks," Physical Review Letters **109**, 100502 (2012), arXiv:1112.2179.

[28] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam, "Quantum cryptography without switching," Physical Review Letters **93**, 170504 (2004), arXiv:quant-ph/0405105.

[29] Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J. Cerf, "Security of continuous-variable quantum key distribution against general attacks," Physical Review Letters **110**, 030502 (2013), arXiv:1208.4920.

[30] Vladyslav C. Usenko and Frédéric Grosshans, "Unidimensional continuous-variable quantum key distribution," Physical Review A **92**, 062337 (2015), arXiv:1504.07093.

[31] Vladyslav C. Usenko and Radim Filip, "Feasibility of continuous-variable quantum key distribution with noisy coherent states," Physical Review A **81**, 022318 (2010), arXiv:0904.1694.

[32] Christian Weedbrook, Stefano Pirandola, Seth Lloyd, and Timothy C. Ralph, "Quantum cryptography approaching the classical limit," Physical Review Letters **105**, 110501 (2010), arXiv:1004.3345.

[33] Jaromír Fiurasek and Nicolas J. Cerf, "Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution," Physical Review A **86**, 060302 (2012), arXiv:1205.6933.

[34] Nathan Walk, Timothy C. Ralph, Thomas Symul, and Ping Koy Lam, "Security of continuous-variable quantum cryptography with Gaussian postselection," Physical Review A **87**, 020303 (2013), arXiv:1206.0936.

[35] Timothy C. Ralph, "Continuous variable quantum cryp-

tography," Physical Review A **61**, 010303 (1999), arXiv:quant-ph/9907073.
[36] Margaret D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," Physical Review A **62**, 062308 (2000), arXiv:quant-ph/9909030.
[37] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, "Quantum cryptography using pulsed homodyne detection," Physical Review A **68**, 042331 (2003), arXiv:quant-ph/0008037.
[38] Yi-Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus, "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks," Physical Review A **79**, 012307 (2009), arXiv:0807.3751.
[39] Kamil Brádler and Christian Weedbrook, "Security proof of continuous-variable quantum key distribution using three coherent states," Physical Review A **97**, 022310 (2018), arXiv:1709.01758.
[40] Anthony Leverrier and Philippe Grangier, "Continuous-variable quantum key distribution protocols with a discrete modulation," (2010), arXiv:1002.4083.
[41] Anthony Leverrier and Philippe Grangier, "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation," Physical Review A **83**, 042312 (2011), arXiv:1101.3008.
[42] Zhengyu Li, Yi-Chen Zhang, and Hong Guo, "User-defined quantum key distribution," ArXiv:1805.04249.
[43] Denis Sych and Gerd Leuchs, "Coherent state quantum key distribution with multi letter phase-shift keying," New Journal of Physics **12**, 053019 (2010), arXiv:0902.1895.
[44] Yihong Wu and Sergio Verdú, "The impact of constellation cardinality on Gaussian channel capacity," in *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)* (2010) pp. 620–628.
[45] Felipe Lacerda, Joseph M. Renes, and Volkher B. Scholz, "Coherent-state constellations and polar codes for thermal Gaussian channels," Physical Review A **95**, 062343 (2017), arXiv:1603.05970.
[46] Maksim E. Shirokov, "Tight uniform continuity bounds for the quantum conditional mutual information, for the Holevo quantity, and for capacities of quantum channels," Journal of Mathematical Physics **58**, 100202 (2017), arXiv:1512.09047.
[47] Paul Jouguet, Sébastien Kunz-Jacques, Eleni Diamanti, and Anthony Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," Physical Review A **86**, 032309 (2012), arXiv:1206.6357.
[48] Shouvik Ghorai, Philippe Grangier, Eleni Diamanti, and Anthony Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," Physical Review X **9**, 021059 (2019), arXiv:1902.01317.
[49] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus, "Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution," Physical Review X **9**, 041064 (2019), arXiv:1905.10896.
[50] The phase symmetrization performed in Steps 2-3 of the protocol implies that Bob need only perform measurements in one quadrature. That is, the effect of phase symmetrization is to symmetrize Eve's attack evenly with respect to both the position and momentum quadratures, and therefore a measurement of only one of the quadratures suffices to detect Eve's tampering. It is for this reason that we have elected to simplify the CV-QKD protocol so that all of the homodyne measurements are conducted with respect to a single quadrature.
[51] Alexander S. Holevo, "Entanglement-assisted capacity of constrained channels," Proceedings of SPIE, First International Symposium on Quantum Informatics **5128**, 62–69 (2003), arXiv:quant-ph/0211170.
[52] Alexander S. Holevo, "Entanglement-assisted capacities of constrained quantum channels," Theory of Probability & Its Applications **48**, 243–255 (2004), arXiv:quant-ph/0211170, http://dx.doi.org/10.1137/S0040585X97980415.
[53] Andreas Winter, "Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints," Communications in Mathematical Physics **347**, 291–313 (2016), arXiv:1507.07775.
[54] Igor Devetak and Andreas Winter, "Distillation of secret key and entanglement from quantum states," Proceedings of the Royal Society A **461**, 207–235 (2005), arXiv:quant-ph/0306078.
[55] Barbara Kraus, Nicolas Gisin, and Renato Renner, "Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication," Physical Review Letters **95**, 080501 (2005), arXiv:quant-ph/0410215.
[56] Frédéric Grosshans and Philippe Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," Proceedings of the 6th International Conference on Quantum Communications, Measurement, and Computing (2002), arXiv:quant-ph/0204127.
[57] Raúl García-Patrón and Nicolas J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," Physical Review Letters **97**, 190503 (2006), arXiv:quant-ph/0608032.
[58] Miguel Navascués, Frédéric Grosshans, and Antonio Acín, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," Physical Review Letters **97**, 190502 (2006), arXiv:quant-ph/0608034.
[59] Michael M. Wolf, Geza Giedke, and J. Ignacio Cirac, "Extremality of Gaussian quantum states," Physical Review Letters **96**, 080502 (2006), arXiv:quant-ph/0509154.
[60] Christopher Gerry and Peter Knight, *Introductory Quantum Optics* (Cambridge University Press, 2004).
[61] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier, "Quantum key distribution over 25km with an all-fiber continuous-variable system," Physical Review A **76**, 042305 (2007), arXiv:0706.4255.
[62] J. Stoer and R. Bulirsch, *Introduction to Numerical Analysis* (Springer New York, 2002).
[63] Kristan Temme, Michael J. Kastoryano, Mary Beth Ruskai, Michael M. Wolf, and Frank Verstraete, "The χ^2–divergence and mixing times of quantum Markov processes," Journal of Mathematical Physics **51**, 122201 (2010), arXiv:1005.2358.
[64] Alessio Serafini, *Quantum Continuous Variables* (CRC Press, 2017).
[65] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes

Hübel, "Continuous–Variable quantum key distribution with Gaussian modulation–The theory of practical implementations," Advanced Quantum Technologies **1**, 1800011 (2018), arXiv:1703.09278.
[66] Filip Rozpędek, Kenneth Goodenough, Jeremy Ribeiro, Norbert Kalb, Valentina Caprara Vivoli, Andreas Reiserer, Ronald Hanson, Stephanie Wehner, and David Elkouss, "Parameter regimes for a single sequential quantum repeater," Quantum Science and Technology **3**, 034002 (2018), arXiv:1705.00043.
[67] Takuya Hirano, Tsubasa Ichikawa, Takuto Matsubara, Motoharu Ono, Yusuke Oguri, Ryo Namiki, Kenta Kasai, Ryutaroh Matsumoto, and Toyohiro Tsurumaru, "Implementation of continuous-variable quantum key distribution with discrete modulation," Quantum Science and Technology **2**, 024010 (2017).
[68] Zhen Qu and Ivan B. Djordjevic, "High-speed continuous-variable quantum key distribution over atmospheric turbulent channels," Proceedings of SPIE **10118**, 101180B (2017).
[69] Jiawei Li, Duan Huang, Cailang Xie, Ling Zhang, and Ying Guo, "Performance improvement of discrete-modulation continuous-variable quantum key distribution by using the machine-learning-based detector," in *Conference on Lasers and Electro-Optics* (Optical Society of America, 2018) p. JTh2A.13.

A. PROOF OF PROPOSITION 1

In this appendix, we provide a proof of Proposition 1. We first restate it here for convenience.

Proposition 2 *Let* $\overline{\rho} = \sum_x r_X(x)\,|\alpha_x\rangle\langle\alpha_x|$, *where*

$$\alpha_x = \frac{q_A + ip_A}{\sqrt{2}}, \tag{106}$$

$$r_X(x) = r_{Q_A}(q_A)\, r_{P_A}(p_A), \tag{107}$$

$$\theta_{N_S} = \int dx\, r_X^G(x)\,|\alpha_x\rangle\langle\alpha_x|\,, \tag{108}$$

and $r^G(x)$ *is the P-function of a thermal state with mean photon number* N_S. *If* $\sqrt{\chi^2(\overline{\rho}, \theta(N_S))} \leq \varepsilon^2$, *and Eve's attacks fulfill the constraints in Section III, then*

$$\gamma_{11} = \gamma_{11}^G, \tag{109}$$

$$|\gamma_{22} - \gamma_{22}^G| \leq \varepsilon_1, \tag{110}$$

$$|\gamma_{12} - \gamma_{12}^G| \leq \varepsilon_2, \tag{111}$$

where

$$\varepsilon_1 = \varepsilon \cdot (1 + c_1) \cdot \sqrt{\mathbb{E}\left[(Q_B - \mathbb{E}[Q_B])^4\right]}, \tag{112}$$

$$\tag{113}$$

for some constant $c_1 > 0$ *and*

$$\begin{aligned}\varepsilon_2 = &\sum_{k=0}^{2m-2}\sum_{l=2m}^{K} \mu_{kl}\left|\eta^G(q_A, k+1)\left(\eta^G(p_A, l) - \eta(p_A, l)\right)\right| \\ &+ \sum_{k=2m-1}^{K}\sum_{l=0}^{2m-1} \mu_{kl}\left|\eta^G(p_A, l)\left(\eta^G(q_A, k+1) - \eta(q_A, k+1)\right)\right| \\ &+ \sum_{k=2m-1, l=2m}^{K} \mu_{kl}\left|\eta^G(p_A, l)\eta^G(q_A, k+1) - \eta(p_A, l)\eta(q_A, k+1)\right|, \end{aligned} \tag{114}$$

where μ_{kl} *is an arbitrary function for* $k \leq 2m-2$, $l \leq 2m-1$ *and is equal to* $\exp(-a(k+l))$ *otherwise. We also have*

$$\eta^G(q_A, k) = \mathbb{E}_{r_{Q_A}^G}[Q_A^k], \tag{115}$$

$$\eta(q_A, k) = \mathbb{E}_{r_{Q_A}}[Q_A^k], \tag{116}$$

$$\eta^G(p_A, k) = \mathbb{E}_{r_{P_A}^G}[P_A^k], \tag{117}$$

$$\eta(p_A, k) = \mathbb{E}_{r_{P_A}}[P_A^k]. \tag{118}$$

Proof. For simplicity, we prove the claim under the assumption that all random variables have zero mean, and we note that it can be generalized by adopting a shift of the variables involved in the proof.

To prove the equality in (109), consider the following: γ_{11} is equal to the variance of the position quadrature that is encoded by Alice during the preparation procedure. Since we are using the Gauss-Hermite approximation of the Gaussian for the encoding, for which the lower moments match those of the Gaussian distribution, it follows that $\gamma_{11} = \gamma_{11}^G$. To prove the inequality in (110), observe that

$$\|\overline{\rho} - \theta(N_S)\|_1 \leq \sqrt{\chi^2(\overline{\rho}, \theta(N_S))} \leq \varepsilon^2, \tag{119}$$

implies that

$$\|\mathcal{N}(\overline{\rho}) - \mathcal{N}(\theta(N_S))\|_1 \leq \varepsilon^2. \tag{120}$$

The inequality in (120) follows from data processing.

Now let us define

$$r_{Q_B}(q_B) \equiv \int\int dx\ dp_B\ W^{\mathcal{N},\alpha_x}(q_B, p_B) r_X(x), \tag{121}$$

$$r^G_{Q_B}(q_B) \equiv \int\int dx\ dp_B\ W^{\mathcal{N},\alpha_x}(q_B, p_B) r^G_X(x), \tag{122}$$

where $W^{\mathcal{N},\alpha_x}$ is the associated Wigner function for the state resulting from transmitting a coherent state over the channel $\mathcal{N}$. Let $r_{Q_B|X}(q_B|x) \equiv \int dp_B\, W^{\mathcal{N},\alpha_x}(q_B, p_B)$ be the probability distribution obtained over the position quadrature when the coherent state α_x is sent over a channel $\mathcal{N}$.

Then we have the following:

$$\int dq_B \left| r_{Q_B}(q_B) - r^G_{Q_B}(q_B) \right| \leq \|\mathcal{N}(\overline{\rho}) - \mathcal{N}(\theta(N_S))\|_1 \leq \varepsilon^2, \tag{123}$$

which is a consequence of monotonicity of trace distance and (119).

We obtain the following:

$$|\gamma^G_{22} - \gamma_{22}| = \left| \int dq_B\ r^G_{Q_B}(q_B)\ |q_B|^2 - \int dq_B\ r_{Q_B}(q_B)\ |q_B|^2 \right| \tag{124}$$

$$= \left| \int dq_B\ \left[r^G_{Q_B}(q_B) - r_{Q_B}(q_B) \right]\ |q_B|^2 \right| \tag{125}$$

$$= \left| \int dq_B\ \left[\sqrt{r^G_{Q_B}(q_B)}\sqrt{r^G_{Q_B}(q_B)} - \sqrt{r^G_{Q_B}(q_B)}\sqrt{r_{Q_B}(q_B)} + \sqrt{r^G_{Q_B}(q_B)}\sqrt{r_{Q_B}(q_B)} - \sqrt{r_{Q_B}(q_B)}\sqrt{r_{Q_B}(q_B)} \right]\ |q_B|^2 \right| \tag{126}$$

$$\leq \int dq_B\ \left| \sqrt{r^G_{Q_B}(q_B)} - \sqrt{r_{Q_B}(q_B)} \right|\ \sqrt{r^G_{Q_B}(q_B)}\, |q_B|^2 + \int dq_B\ \left| \sqrt{r^G_{Q_B}(q_B)} - \sqrt{r_{Q_B}(q_B)} \right|\ \sqrt{r_{Q_B}(q_B)}\, |q_B|^2 \tag{127}$$

$$\leq \sqrt{\int dq_B\ \left| \sqrt{r^G_{Q_B}(q_B)} - \sqrt{r_{Q_B}(q_B)} \right|^2 \int dq_B\ r^G_{Q_B}(q_B)\, |q_B|^4} + \sqrt{\int dq_B\ \left| \sqrt{r^G_{Q_B}(q_B)} - \sqrt{r_{Q_B}(q_B)} \right|^2 \int dq_B\ r_{Q_B}(q_B)\, |q_B|^4} \tag{128}$$

$$= \sqrt{\int dq_B\ \left| \sqrt{r^G_{Q_B}(q_B)} - \sqrt{r_{Q_B}(q_B)} \right|^2} \left(\sqrt{\int dq_B\ r^G_{Q_B}(q_B)\, |q_B|^4} + \sqrt{\int dq_B\ r_{Q_B}(q_B)\, |q_B|^4} \right). \tag{129}$$

Now using that $\sqrt{\int dq_B \left| \sqrt{r^G_{Q_B}(q_B)} - \sqrt{r_{Q_B}(q_B)} \right|^2}$ is the Hellinger divergence and less than the square root of the total variation distance $\int dq_B \left| r^G_{Q_B}(q_B) - r_{Q_B}(q_B) \right|$, we obtain that

$$\left| \int dq_B\ r^G_{Q_B}(q_B)\ |q_B|^2 - \int dq_B\ r_{Q_B}(q_B)\ |q_B|^2 \right| \leq \varepsilon \cdot \left(\sqrt{\int dq_B\ r^G_{Q_B}(q_B)\, |q_B|^4} + \sqrt{\int dq_B\ r_{Q_B}(q_B)\, |q_B|^4} \right). \tag{130}$$

To bound the second term we invoke the assumption that the photon number variance of the channel output is bounded. Therefore,

$$\mathrm{Tr}(\hat{n}^2\rho) = \mathrm{Tr}\left((\hat{q}_B^2 + \hat{p}_B^2 - 1)^2\rho\right) \tag{131}$$

$$= \mathrm{Tr}\left((\hat{q}_B^4 + \hat{p}_B^4 + 1 - 2\hat{q}_B^2 - 2\hat{p}_B^2 + 2\hat{q}_B^2\hat{p}_B^2)\rho\right) < \infty, \tag{132}$$

where $\rho = \mathcal{N}\left(\theta(N_S)\right)$. We thus conclude that $\sqrt{\int dq_B\ r^G_{Q_B}(q_B)\,|q_B|^4}$ is also bounded, so that $\sqrt{\int dq_B\ r^G_{Q_B}(q_B)\,|q_B|^4} \leq c_1 \cdot \sqrt{\int dq_B\ r_{Q_B}(q_B)\,|q_B|^4}$, for some constant $c_1 > 0$.

To prove the inequality in (111), observe the following:

$$\gamma_{12} = \int\int dq_A\ dp_A\ r_{Q_A}(q_A)\ r_{P_A}(p_A) q_A \int\int dp_B\ dq_B\ r_{Q_B,P_B|Q_A,P_A}(q_B\ p_B|q_A\ p_A) q_B. \tag{133}$$

$$= \int\int dq_A\ dp_A\ r_{Q_A}(q_A)\ r_{P_A}(p_A) q_A \int dq_B\ r_{Q_B|Q_A,P_A}(q_B|q_A\ p_A) q_B. \tag{134}$$

Let us define

$$\mu(q_A, p_A) \equiv \int dq_B\ q_B\ r_{Q_B|Q_A P_A}(q_B|q_A p_A). \tag{135}$$

This implies that

$$\gamma_{12} = \int\int dq_A\ dp_A\ r_{Q_A}(q_A)\ r_{P_A}(p_A)\ q_A\ \mu(q_A, p_A). \tag{136}$$

Similarly, we can define

$$\gamma^G_{12} = \int\int dq_A\ dp_A\ r^G_{Q_A}(q_A)\ r^G_{P_A}(p_A)\ q_A\ \mu(q_A, p_A). \tag{137}$$

This implies

$$|\gamma_{12} - \gamma^G_{12}| = \left| \int dq_A\ dp_A\ \mu(q_A, p_A)\left(r^G(p_A)\ r^G(q_A) q_A - r_{P_A}(p_A)\ r_{Q_A}(q_A) q_A\right)\right|. \tag{138}$$

Now let us suppose that it is possible to expand $\mu(q_A, p_A)$ as a polynomial in q_A and p_A, as mentioned in the assumptions from Section III. That is,

$$\mu(q_A, p_A) = \sum_{k=0}^{K}\sum_{l=0}^{K} \mu_{k,l} q_A^k p_A^l. \tag{139}$$

This assumption implies that the mean value of Bob's position-quadrature measurement result when a coherent state $|\alpha(q_A, p_A)\rangle\langle\alpha(q_A, p_A)|$ is transmitted through an unknown channel $\mathcal{N}$ is no more than polynomial in q_A and p_A.

With this assumption, we obtain the following:

$$|\gamma_{12} - \gamma^G_{12}| = \left| \sum_{k,l} \mu_{k,l} \int\int dq_A\ dp_A \left(r^G_{P_A}(p_A)\ p_A^l\ r^G_{Q_A}(q_A)\ q_A^{k+1} - r_{P_A}(p_A)\ p_A^l\ r_{Q_A}(q_A)\ q_A^{k+1}\right)\right| \tag{140}$$

Let us now define the following:

$$\eta^G(p_A, l) \equiv \int dp_A\ r^G_{P_A}(p_A)\ p_A^l, \tag{141}$$

$$\eta^G(q_A, l) \equiv \int dq_A\ r^G_{Q_A}(q_A)\ q_A^l, \tag{142}$$

$$\eta(p_A, l) \equiv \int dp_A\ r_{P_A}(p_A)\ p_A^l, \tag{143}$$

$$\eta(q_A, l) \equiv \int dq_A\ r_{Q_A}(p_A)\ q_A^l. \tag{144}$$

This implies that

$$|\gamma_{12} - \gamma_{12}^G| \leq \sum_{k,l} \mu_{k,l} \left| \eta^G(p_A, l)\eta^G(q_A, k+1) - \eta(p_A, l)\eta(q_A, k+1) \right| \tag{145}$$

Now, we know that the first $2m-1$ moments of the Gauss-Hermite distribution are equal to the first $2m-1$ moments of the Gaussian distribution. With that, we conclude the following upper bound:

$$\begin{aligned} |\gamma_{12} - \gamma_{12}^G| \leq & \sum_{k=0}^{2m-2} \sum_{l=2m}^{K} \mu_{kl} \left| \eta^G(q_A, k+1) \left(\eta^G(p_A, l) - \eta(p_A, l) \right) \right| \\ & + \sum_{k=2m-1}^{K} \sum_{l=0}^{2m-1} \mu_{kl} \left| \eta^G(p_A, l) \left(\eta^G(q_A, k+1) - \eta(q_A, k+1) \right) \right| \\ & + \sum_{k=2m-1, l=2m}^{K} \mu_{kl} \left| \eta^G(p_A, l)\eta^G(q_A, k+1) - \eta(p_A, l)\eta(q_A, k+1) \right|. \end{aligned} \tag{146}$$

This concludes the proof. ■

B. CHANNEL SYMMETRIZATION

We now show that by performing a discrete phase symmetrization in Steps 2-3 of the key distribution protocol from Section II, it is possible to simplify the form of the covariance matrix of the state that Alice and Bob share at the end of the EB protocol to a symmetrized form.

Let $\mathcal{N}_{A\to B}$ be a single-mode bosonic channel. Alice and Bob can make this channel phase covariant by applying a random phase rotation and its inverse at the channel input and output, respectively, resulting in the following symmetrized channel:

$$\overline{\mathcal{N}}_{A\to B}(\rho_A) = \frac{1}{4} \sum_{k=0}^{3} e^{i\hat{n}_B \pi k/2} \mathcal{N}_{A\to B}(e^{-i\hat{n}_A \pi k/2} \rho_A e^{i\hat{n}_A \pi k/2}) e^{-i\hat{n}_B \pi k/2}. \tag{147}$$

If the state input to the phase randomized channel is one share of a two-mode squeezed vacuum $\psi(\bar{n})_{RA} = |\psi(\bar{n})\rangle\langle\psi(\bar{n})|_{RA}$, defined from

$$|\psi(\bar{n})\rangle_{RA} \equiv \frac{1}{\sqrt{\bar{n}+1}} \sum_{n=0}^{\infty} \sqrt{\left(\frac{\bar{n}}{\bar{n}+1} \right)^n} |n\rangle_R \otimes |n\rangle_A, \tag{148}$$

then it follows that

$$\overline{\mathcal{N}}_{A\to B}(\psi(\bar{n})_{RA}) = \frac{1}{4} \sum_{k=0}^{3} \left(e^{-i\hat{n}_R \pi k/2} \otimes e^{i\hat{n}_B \pi k/2} \right) \mathcal{N}_{A\to B}(\psi(\bar{n})_{RA}) \left(e^{i\hat{n}_R \pi k/2} \otimes e^{-i\hat{n}_B \pi k/2} \right), \tag{149}$$

where we have applied the fact that

$$e^{-i\hat{n}_A \pi k/2} |\psi(\bar{n})\rangle_{RA} = e^{-i\hat{n}_R \pi k/2} |\psi(\bar{n})\rangle_{RA}. \tag{150}$$

We would now like to determine the covariance matrix elements of the phase-randomized state $\tau_{RB} \equiv \overline{\mathcal{N}}_{A\to B}(\psi(\bar{n})_{RA})$:

$$\begin{bmatrix} 2\langle \hat{x}_R^2 \rangle_\tau & \langle\{\hat{x}_R, \hat{p}_R\}\rangle_\tau & \langle\{\hat{x}_R, \hat{x}_B\}\rangle_\tau & \langle\{\hat{x}_R, \hat{p}_B\}\rangle_\tau \\ \langle\{\hat{x}_R, \hat{p}_R\}\rangle_\tau & 2\langle \hat{p}_R^2 \rangle_\tau & \langle\{\hat{p}_R, \hat{x}_B\}\rangle_\tau & \langle\{\hat{p}_R, \hat{p}_B\}\rangle_\tau \\ \langle\{\hat{x}_R, \hat{x}_B\}\rangle_\tau & \langle\{\hat{p}_R, \hat{x}_B\}\rangle_\tau & 2\langle \hat{x}_B^2 \rangle_\tau & \langle\{\hat{x}_B, \hat{p}_B\}\rangle_\tau \\ \langle\{\hat{x}_R, \hat{p}_B\}\rangle_\tau & \langle\{\hat{p}_R, \hat{p}_B\}\rangle_\tau & \langle\{\hat{x}_B, \hat{p}_B\}\rangle_\tau & 2\langle \hat{p}_B^2 \rangle_\tau \end{bmatrix}, \tag{151}$$

where we assume for simplicity that τ_{RB} has zero mean, but we note here that the more general case can be incorporated by a shift. Given an initial covariance matrix with elements

$$\sigma = \begin{bmatrix} \sigma_{11} & \sigma_{12} & \sigma_{13} & \sigma_{14} \\ \sigma_{12} & \sigma_{22} & \sigma_{23} & \sigma_{24} \\ \sigma_{13} & \sigma_{23} & \sigma_{33} & \sigma_{34} \\ \sigma_{14} & \sigma_{24} & \sigma_{34} & \sigma_{44} \end{bmatrix}, \tag{152}$$

the phase rotation $e^{-i\hat{n}_R\phi} \otimes e^{i\hat{n}_B\phi}$ corresponds to the following symplectic transformation

$$X(\phi) = \begin{bmatrix} \cos(\phi) & \sin(\phi) & 0 & 0 \\ -\sin(\phi) & \cos(\phi) & 0 & 0 \\ 0 & 0 & \cos(\phi) & -\sin(\phi) \\ 0 & 0 & \sin(\phi) & \cos(\phi) \end{bmatrix}. \tag{153}$$

So then calculating covariance matrix for the phase randomized state, it is given by

$$\frac{1}{4}\sum_{k=0}^{3} X(\pi k/2)\sigma X^T(\pi k/2), \tag{154}$$

and we find that it is equal to

$$\frac{1}{2}\begin{bmatrix} \sigma_{11}+\sigma_{22} & 0 & \sigma_{13}-\sigma_{24} & \sigma_{14}+\sigma_{23} \\ 0 & \sigma_{11}+\sigma_{22} & \sigma_{14}+\sigma_{23} & -(\sigma_{13}-\sigma_{24}) \\ \sigma_{13}-\sigma_{24} & \sigma_{14}+\sigma_{23} & \sigma_{33}+\sigma_{44} & 0 \\ \sigma_{14}+\sigma_{23} & -(\sigma_{13}-\sigma_{24}) & 0 & \sigma_{33}+\sigma_{44} \end{bmatrix}. \tag{155}$$

The latter has the following form:

$$\begin{bmatrix} a & 0 & c_2 & c_1 \\ 0 & a & c_1 & -c_2 \\ c_2 & c_1 & b & 0 \\ c_1 & -c_2 & 0 & b \end{bmatrix}, \tag{156}$$

for $a, b \geq 1$ and $c_1, c_2 \in \mathbb{R}$. We can write this in the form of Eq. (D34) in [25] by setting $c_1 = z\sin(\theta)$ and $c_2 = z\cos(\theta)$, so that $z = \sqrt{c_1^2 + c_2^2}$ and $\theta = \arctan(c_1/c_2)$, so that the form becomes

$$\begin{bmatrix} a & 0 & z\cos(\theta) & z\sin(\theta) \\ 0 & a & z\sin(\theta) & -z\cos(\theta) \\ z\cos(\theta) & z\sin(\theta) & b & 0 \\ z\sin(\theta) & -z\cos(\theta) & 0 & b \end{bmatrix} = \begin{bmatrix} a\mathbb{I}_2 & z\,R(\theta) \\ z\,R(\theta) & b\mathbb{I}_2 \end{bmatrix}. \tag{157}$$

This completes the symmetrization of the covariance matrix due to the discrete phase randomization.

Ideally, we would estimate all the elements of the covariance matrix in the channel estimation step of the protocol. However, it is much simpler to estimate only the parameters a, b, and $z\cos(\theta)$, and assume instead that the covariance matrix has the following form:

$$\begin{bmatrix} a & 0 & z\cos(\theta) & 0 \\ 0 & a & 0 & -z\cos(\theta) \\ z\cos(\theta) & 0 & b & 0 \\ 0 & -z\cos(\theta) & 0 & b \end{bmatrix}. \tag{158}$$

That is, we ignore all correlations between position and momentum quadratures. The effect of doing so is to underestimate the correlations that are present in the state τ_{RB}. Therefore, this intuitively means we overestimate Eve's Holevo information during the channel estimation phase, and exhaustive numerical checks confirm that Eve's Holevo information is larger when replacing z with $z\cos(\theta)$ (as was reported in [25]). Since we overestimate the Holevo information, the security of the protocol is not compromised, but it is only the final key rate that is potentially reduced. For additional discussion, see Appendix D of [25].

C. ALTERNATIVE APPROACH FOR BOUNDING THE PARAMETERS OF A HYPOTHETICAL GAUSSIAN-MODULATED PROTOCOL

In this section, we outline a method to remove the parameters c_1 and c_2 from the security proof of discrete-modulation protocols.

Let $\overline{\rho}$ be the averaged state that Alice sends to Bob in the discrete-modulation protocol, and let the thermal state $\theta(N_S)$ be the averaged state that Alice sends to Bob in Gaussian-modulation protocol. Let $\mathcal{S}$ be a set of isometries $\mathcal{U}_{A\to BE}$ that Eve implements and which agrees with the statistics that are collected by Alice and Bob, and fullfills the

criteria given in Section III. Then, we want to obtain an upper bound on the Holevo information $\sup_{\mathcal{U}\in\mathcal{S}} \chi(B;E)_{\mathcal{U}(\overline{\rho})}$. Let $\mathcal{W} = \text{Span}\left\{|\alpha_1\rangle, |\alpha_2\rangle, \ldots |\alpha_{m^2}\rangle\right\}$ be a finite-dimensional vector space, and is spanned by a basis having m^2 elements. We want to construct an orthonormal basis for this space, and this can be done by using Gram-Schmidt orthogonalization method. Let

$$|\phi_i'\rangle = |\alpha_i\rangle - \sum_{j=1}^{i-1} \langle\phi_j'|\alpha_i\rangle |\phi_j'\rangle, \tag{159}$$

and define $|\phi_i\rangle = \frac{|\phi_i'\rangle}{\|\phi_i'\|}$. We can then construct the following orthonormal basis $\{|\phi_1\rangle, |\phi_2\rangle \ldots |\phi\rangle_{m^2}\}$ for $\mathcal{W}$. Now, let us define the following projector on $\mathcal{W}$:

$$\Pi_W = \sum_{i=1}^{m^2} |\phi_i\rangle\langle\phi_i|. \tag{160}$$

It is easy to see that

$$\Pi_W \overline{\rho} \Pi_W = \overline{\rho}. \tag{161}$$

To each isometry $\mathcal{U}_{A'\to BE} \in \mathcal{S}$, we can define the following isometry $\overline{\mathcal{U}}$ such that

$$\text{Tr}_{E'}\left[\overline{\mathcal{U}}_{A'\to BEE'}(\rho_{A'})\right] = \mathcal{U}_{A'\to BE}(\Pi_W \rho_{A'} \Pi_W) + \text{Tr}\left[(1-\Pi_W)\rho_{A'}\right]|u\rangle\langle u|_{BE}, \tag{162}$$

where $|u\rangle_{BE}$ is an arbitrary unit vector in $\mathcal{H}_{BE}$. Then, $\text{Tr}_{E'}\left[\overline{\mathcal{U}}_{A'\to BEE'}(\overline{\rho}_{A'})\right] = \mathcal{U}_{A'\to BE}(\Pi_W \overline{\rho}_{A'} \Pi_W)$. We also have that

$$\chi(B;EE')_{\overline{\mathcal{U}}(\bar{\rho})} \geq \chi(B;E)_{\overline{\mathcal{U}}(\bar{\rho})} = \chi(B;E)_{\mathcal{U}(\bar{\rho})} \tag{163}$$

Then, using the continuity of Holevo information, we obtain

$$\chi(B;E)_{\overline{\mathcal{U}}(\bar{\rho})} \leq \chi(B;EE')_{\overline{\mathcal{U}}(\theta(N_S))} + f(\varepsilon, N_S), \tag{164}$$

where $f(\varepsilon, N_s)$ is defined in (38). Now we need to obtain an upper bound on $\chi(B;EE')_{\overline{\mathcal{U}}(\theta(N_S))}$. This Holevo information is calculated for a thermal state $\theta(N_S)$ sent over an isometric channel $\overline{\mathcal{U}}_{A'\to BEE'}$ in the set $\mathcal{S}$ and Bob performing homodyne or heterodyne measurement. For this, we obtain the parameters $\bar{\gamma}_{11}^G, \bar{\gamma}_{12}^G$ and $\bar{\gamma}_{22}^G$, which are defined analogously to (49)–(51), with the initial random variable Q_A replaced with Gaussian random variable with mean zero and variance equal to N_S. In the following proposition, we obtain bounds on the parameters $\bar{\gamma}_{11}^G, \bar{\gamma}_{12}^G$ and $\bar{\gamma}_{22}^G$ with respect to γ_{11}, γ_{12}, and γ_{22} observed in discrete-modulation protocol.

Proposition 3 *Let $\overline{\rho} = \sum_x r_X(x)|\alpha_x\rangle\langle\alpha_x|$, where*

$$\alpha_x = \frac{q_{A_s} + ip_{A_t}}{\sqrt{2}}, \tag{165}$$

$$r_X(x) = r_{Q_A}(q_{A_s})\, r_{P_A}(p_{A_t}), \tag{166}$$

$$\theta_{N_S} = \int dx\, r^G(x)|\alpha_x\rangle\langle\alpha_x|, \tag{167}$$

where $r^G(x)$ is the P-function for a thermal state with mean photon number N_S, and $s,t \in \{1\cdots m\}$. If $\sqrt{\chi^2(\overline{\rho}, \theta(N_S))} \leq \varepsilon^2$ and Eve's attack $\mathcal{U}_{A'\to B'E'}$ fulfills the constraints in Section III, then,

$$\bar{\gamma}_{11}^G = \gamma_{11}, \tag{168}$$

$$\bar{\gamma}_{22}^G \leq \gamma_{22} + \gamma_{22}\left\|\overline{\rho}^{(-\frac{1}{2})}\right\|_\infty^2 \varepsilon + \varepsilon\,\text{Tr}\left[|u\rangle\langle u|\,\hat{q}^2\right], \tag{169}$$

$$\bar{\gamma}_{12}^G \geq z\gamma_{12} + \int dq_A r^G(q_A) q_A \int dp_A r^G(p_A)\,\text{Tr}\left[(\mathbb{I}-\Pi_W)|\alpha(q_A,p_A)\rangle\langle\alpha(q_A,p_A)|\right]\text{Tr}\left[|u\rangle\langle u|\,\hat{q}\right], \tag{170}$$

where $\Pi_W = \sum_{i=1}^{m^2}|\phi_i\rangle\langle\phi_i|$, $|u\rangle$ represents an arbitrary unit vector and $|\phi_i\rangle$ with $i \in \left\{1, \cdots m^2\right\}$, forms an orthonormal basis for $\mathcal{W} = \text{Span}\left\{|\alpha_1\rangle, |\alpha_2\rangle, \ldots |\alpha_{m^2}\rangle\right\}$, and

$$z = \min_{i,j}\left|\frac{\int dq_A \int dp_A r^G(q_A) r^G(p_A) q_A d_{ij}(q_A,p_A)}{\sum_{s,t} q_{A_s} r(q_{A_s}) r(p_{A_t}) b_{ij}(s,t)}\right|, \tag{171}$$

with $d_{ij}(q_A,p_A) = \langle\phi_i|\alpha(q_A,p_A)\rangle\langle\alpha(q_A,p_A)|\phi_j\rangle$, and $b_{ij}(s,t) = \langle\phi_i|\alpha(q_{A_s},p_{A_t})\rangle\langle\alpha(q_{A_s},p_{A_t})|\phi_j\rangle$.

Proof. First, consider $\bar{\gamma}_{22}^{G}$ defined as

$$\bar{\gamma}_{22}^{G} = \mathrm{Tr}\left[\hat{q}^2 \mathcal{N}(\Pi_W \theta(N_S) \Pi_W)\right] + \mathrm{Tr}\left[(1-\Pi_W)\left(\theta(N_S)\right)\right] \mathrm{Tr}\left[|u\rangle\langle u|\, \hat{q}^2\right]. \tag{172}$$

Let us concentrate on the first term $\mathrm{Tr}\left[\hat{q}^2 \mathcal{N}(\Pi_W \theta(N_S) \Pi_W)\right] = \mathrm{Tr}\left[\hat{q}^2 \mathcal{N}(\sigma)\right]$, where $\sigma = \Pi_W \theta(N_S) \Pi_W$. Then,

$$\begin{aligned}
\mathrm{Tr}\left[\hat{q}^2 \mathcal{N}(\sigma)\right] &= \mathrm{Tr}\left[\hat{q}^2 \mathcal{N}(\overline{\rho}^{(\frac{1}{2})} \overline{\rho}^{(-\frac{1}{2})} \sigma \overline{\rho}^{(-\frac{1}{2})} \overline{\rho}^{(\frac{1}{2})})\right] && (173)\\
&\leq \mathrm{Tr}\left[\hat{q}^2 \mathcal{N}(\overline{\rho})\right] \|\overline{\rho}^{(-\frac{1}{2})} \sigma \overline{\rho}^{(-\frac{1}{2})}\|_\infty && (174)\\
&\leq \gamma_{22} \|\overline{\rho}^{(-\frac{1}{2})} \sigma \overline{\rho}^{(-\frac{1}{2})}\|_\infty. && (175)
\end{aligned}$$

To obtain (174) from (173), observe that

$$\begin{aligned}
\rho^{-1/2} \sigma \rho^{-1/2} &\leq \|\rho^{-1/2} \sigma \rho^{-1/2}\|_\infty\, I && (176)\\
\implies \rho^{1/2} \rho^{-1/2} \sigma \rho^{-1/2} \rho^{1/2} &\leq \|\rho^{-1/2} \sigma \rho^{-1/2}\|_\infty\, \rho && (177)\\
\implies \mathrm{Tr}\left[\hat{q}^2 \rho^{1/2} \rho^{-1/2} \sigma \rho^{-1/2} \rho^{1/2}\right] &\leq \|\rho^{-1/2} \sigma \rho^{-1/2}\|_\infty \mathrm{Tr}\left[\hat{q}^2 \rho\right] && (178)
\end{aligned}$$

Then, from linearity of channel, the inequality follows.

Now, we would like to obtain an upper bound on $\|\overline{\rho}^{(-\frac{1}{2})} \sigma \overline{\rho}^{(-\frac{1}{2})}\|_\infty$. Let $\Delta = \sigma - \overline{\rho}$. Then,

$$\begin{aligned}
\|\overline{\rho}^{(-\frac{1}{2})} \sigma \overline{\rho}^{(-\frac{1}{2})}\|_\infty &= \|\overline{\rho}^{(-\frac{1}{2})} (\Delta + \overline{\rho}) \overline{\rho}^{(-\frac{1}{2})}\|_\infty && (179)\\
&= \|\overline{\rho}^{(-\frac{1}{2})} \Delta \overline{\rho}^{(-\frac{1}{2})} + \mathbb{I}\|_\infty && (180)\\
&\leq \|\mathbb{I}\|_\infty + \|\overline{\rho}^{(-\frac{1}{2})} \Delta \overline{\rho}^{(-\frac{1}{2})}\|_\infty && (181)\\
&\leq 1 + \|\overline{\rho}^{(-\frac{1}{2})}\|_\infty^2 \|\Delta\|_\infty && (182)\\
&\leq 1 + \|\overline{\rho}^{(-\frac{1}{2})}\|_\infty^2 \|\Delta\|_1. && (183)
\end{aligned}$$

Now, $\|\overline{\rho} - \theta(N_S)\|_1 \leq \varepsilon$. By data-processing we obtain

$$\|\overline{\rho} - \sigma\|_1 \leq \varepsilon. \tag{184}$$

We thus obtain

$$\begin{aligned}
\mathrm{Tr}\left[\hat{q}^2 \mathcal{N}(\sigma)\right] &\leq \gamma_{22} + \gamma_{22} \|\overline{\rho}^{(-\frac{1}{2})}\|_\infty^2 \|\Delta\|_1, && (185)\\
&\leq \gamma_{22} + \gamma_{22} \|\overline{\rho}^{(-\frac{1}{2})}\|_\infty^2 \varepsilon. && (186)
\end{aligned}$$

Now, consider the following term: $\mathrm{Tr}\left[(\mathbb{I} - \Pi_W)\, \theta(N_S)\right]$. We know that

$$\|\overline{\rho} - \theta(N_S)\|_1 \leq \varepsilon \tag{187}$$

This implies,

$$\sup_{0 \leq M \leq 1} \mathrm{Tr}\left[M\, (\theta(N_S) - \overline{\rho})\right] \leq \varepsilon. \tag{188}$$

Choosing $M = \mathbb{I} - \Pi_W$, we obtain, $\mathrm{Tr}\left[(\mathbb{I} - \Pi_W)\, \theta(N_S)\right] \leq \varepsilon$. Then,

$$\bar{\gamma}_{22}^{G} \leq \gamma_{22} + \gamma_{22} \|\overline{\rho}^{(-\frac{1}{2})}\|_\infty^2 \varepsilon + \varepsilon\, \mathrm{Tr}\left[|u\rangle\langle u|\, \hat{q}^2\right]. \tag{189}$$

Now, let us consider the parameter $\bar{\gamma}_{12}^{G}$. Numerical checks, similar to those stated in [40], reveal that Holevo information is a monotonically decreasing function of this parameter. Since we want an upper bound on the Holevo information, we obtain a lower bound on this parameter. First, consider $\bar{\gamma}_{12}^{G,1}$ defined as follows:

$$\begin{aligned}
\bar{\gamma}_{12}^{G,1} &= \int dq_A\; r^G(q_A)\; q_A \int dp_A r^G(p_A) \int dq_B\, \mathrm{Tr}\left[\mathcal{N}\left(\Pi_W\, |\alpha(q_A, p_A)\rangle\langle\alpha(q_A, p_A)|\, \Pi_W\right) \hat{q}_B\right] && (190)\\
&= \int dq_A\; r^G(q_A)\; q_A \int dp_A r^G(p_A) \int dq_B\, \mathrm{Tr}\left[\mathcal{N}\left(\sum_{i,j} d_{ij}(q_A, p_A)\, |\phi_i\rangle\langle\phi_j|\right) \hat{q}_B\right] && (191)
\end{aligned}$$

$$= \int dq_A \; r^G(q_A) \; q_A \int dp_A r^G(p_A) \sum_{i,j} d_{ij}(q_A, p_A) \int dq_B \, \mathrm{Tr}\left[\mathcal{N}\left(|\phi_i\rangle\langle\phi_j|\right) \hat{q}_B\right] \tag{192}$$

$$= \sum_{i,j} \int dq_A \; r^G(q_A) \; q_A \int dp_A r^G(p_A) d_{ij}(q_A, p_A) \int dq_B \, \mathrm{Tr}\left[\mathcal{N}\left(|\phi_i\rangle\langle\phi_j|\right) \hat{q}_B\right] \tag{193}$$

$$= \sum_{i,j} f_{ij} \int dq_B \, \mathrm{Tr}\left[\mathcal{N}\left(|\phi_i\rangle\langle\phi_j|\right) \hat{q}_B\right], \tag{194}$$

where $d_{ij}(q_A, p_A) = \langle\phi_i|\alpha(q_A, p_A)\rangle \langle\alpha(q_A, p_A)|\phi_j\rangle$, and $f_{ij} = \int dq_A \int dp_A r^G(q_A) r^G(p_A) q_A d_{ij}(q_A p_A)$. We can write γ_{12} defined in (50) as

$$\gamma_{12} = \sum_{s,t} q_{A_s} r(q_{A_s}) r(p_{A_t}) \, \mathrm{Tr}\left[\mathcal{N}\left(|\alpha(q_{A_s}, p_{A_t})\rangle\langle\alpha(q_{A_s}, p_{A_t})|\right) \hat{q}_B\right] \tag{195}$$

$$= \sum_{s,t} q_{A_s} r(q_{A_s}) r(p_{A_t}) \, \mathrm{Tr}\left[\sum_{i,j} b_{ij}(s,t) \mathcal{N}\left(|\phi_i\rangle\langle\phi_j|\right) \hat{q}_B\right] \tag{196}$$

$$= \sum_{i,j} \sum_{s,t} q_{A_s} r(q_{A_s}) r(p_{A_t}) b_{ij}(s,t) \, \mathrm{Tr}\left[\mathcal{N}\left(|\phi_i\rangle\langle\phi_j|\right) \hat{q}_B\right] \tag{197}$$

$$= \sum_{i,j} g_{ij} \, \mathrm{Tr}\left[\mathcal{N}\left(|\phi_i\rangle\langle\phi_j|\right) \hat{q}_B\right], \tag{198}$$

where $b_{ij}(s,t) = \langle\phi_i|\alpha(q_{A_s}, p_{A_t})\rangle \langle\alpha(q_{A_s}, p_{A_t})|\phi_j\rangle$, and $g_{ij} = \sum_{s,t} q_{A_s} r(q_{A_s}) r(p_{A_t}) b_{ij}(s,t)$. We can then express $\bar{\gamma}_{12}^{G,1}$ in terms of $\bar{\gamma}_{12}$ as follows:

$$\bar{\gamma}_{12}^{G,1} = \sum_{i,j} \frac{f_{ij}}{g_{ij}} g_{ij} \, \mathrm{Tr}\left[\mathcal{N}\left(|\phi_i\rangle\langle\phi_j|\right) \hat{q}_B\right] \tag{199}$$

$$\geq z \; \gamma_{12}, \tag{200}$$

where $z = \min_{i,j} \left|\frac{f_{ij}}{g_{ij}}\right|$. Let us now define $\bar{\gamma}_{12}^{G,2}$ as

$$\bar{\gamma}_{12}^{G,2} = \int dq_A r^G(q_A) q_A \int dp_A r^G(p_A) \, \mathrm{Tr}\left[\left(\mathbb{I} - \Pi_W\right) |\alpha(q_A, p_A)\rangle\langle\alpha(q_A, p_A)|\right] \mathrm{Tr}\left[|u\rangle\langle u| \, \hat{q}_B\right]. \tag{201}$$

We can calculate the above term numerically.

We can now combine (200) and (201) to obtain the following lower bound on $\bar{\gamma}_{12}^{G} = \bar{\gamma}_{12}^{G,1} + \bar{\gamma}_{12}^{G,2}$:

$$\bar{\gamma}_{12}^{G} \geq z\gamma_{12} + \int dq_A r^G(q_A) q_A \int dp_A r^G(p_A) \, \mathrm{Tr}\left[\left(\mathbb{I} - \Pi_W\right) |\alpha(q_A, p_A)\rangle\langle\alpha(q_A, p_A)|\right) \mathrm{Tr}\left(|u\rangle\langle u| \, \hat{q}_B\right]. \tag{202}$$

This concludes the proof. ■

Corollary 4 *Let* $\overline{\rho} = \sum_x r_X(x) \, |\alpha_x\rangle\langle\alpha_x|$, *where*

$$\alpha_x = \frac{q_{A_s} + i p_{A_t}}{\sqrt{2}}, \tag{203}$$

$$r_X(x) = r_{Q_A}(q_{A_s}) \, r_{P_A}(p_{A_t}), \tag{204}$$

$$\theta_{N_S} = \int dx \, r^G(x) \, |\alpha_x\rangle\langle\alpha_x| \, , \tag{205}$$

where $r^G(x)$ *is the P-function for a thermal state with mean photon number* N_S, *and* $s, t \in \{1 \cdots m\}$. *If* $\sqrt{\chi^2(\overline{\rho}, \theta(N_S))} \leq \varepsilon^2$ *and Eve's attack* $\mathcal{U}_{A' \to B'E'}$ *fulfills the constraints in Section III, then,*

$$\bar{\gamma}_{11}^{G} = \gamma_{11}, \tag{206}$$

$$\bar{\gamma}_{22}^{G} \leq \gamma_{22} + \gamma_{22} \left\| \overline{\rho}^{(-\frac{1}{2})} \right\|_{\infty}^{2} \varepsilon, \tag{207}$$

$$\bar{\gamma}_{12}^{G} \geq z\gamma_{12}, \tag{208}$$

where $\Pi_W = \sum_{i=1}^{m^2} |\phi_i\rangle\langle\phi_i|$ *and* $|\phi_i\rangle$ *with* $i \in \{1, \cdots m^2\}$, *forms an orthonormal basis for* $\mathcal{W} = \text{Span}\{|\alpha_1\rangle, |\alpha_2\rangle, \ldots |\alpha_{m^2}\rangle\}$, *and*

$$z = \min_{i,j} \left| \frac{\int dq_A \int dp_A r^G(q_A) r^G(p_A) q_A d_{ij}(q_A, p_A)}{\sum_{s,t} q_{A_s} r(q_{A_s}) r(p_{A_t}) b_{ij}(s,t)} \right|, \tag{209}$$

with $d_{ij}(q_A, p_A) = \langle\phi_i|\alpha(q_A, p_A)\rangle \langle\alpha(q_A, p_A)|\phi_j\rangle$, *and* $b_{ij}(s,t) = \langle\phi_i|\alpha(q_{A_s}, p_{A_t})\rangle \langle\alpha(q_{A_s}, p_{A_t})|\phi_j\rangle$.

Proof. In Proposition 3, choose $|u\rangle$ to be in the kernel of $\hat{q}$ (for example, a position-squeezed vacuum state that converges to a position eigenstate). ■

In Proposition 3, we obtain a lower bound on $\bar{\gamma}_{12}^{G}$ and upper bound on $\bar{\gamma}_{22}^{G}$. Now, we can follow the steps stated in Section V to obtain an upper bound on $\chi(B;E)_{\overline{\mathcal{U}}(\theta(N_S))}$. Consider a state $\sigma_{ABEE'} = \text{Tr}\left[\overline{\mathcal{U}}_{A'\to BEE'}(\psi(\bar{n}))_{AA'}\right]$, where $|\psi(\bar{n})\rangle_{AA'}$ is TMSV as defined in (69). Let the covariance matrix of σ_{AB} be

$$\begin{bmatrix} \bar{\gamma}_{11}^{\text{EB}} \mathbb{I}_2 & \bar{\gamma}_{12}^{\text{EB}} \sigma_Z \\ \bar{\gamma}_{12}^{\text{EB}} \sigma_Z & \bar{\gamma}_{22}^{\text{EB}} \mathbb{I}_2 \end{bmatrix}. \tag{210}$$

We can use the "PM to EB" mapping defined in Section V B to obtain bounds on parameters $\bar{\gamma}_{11}^{\text{EB}}$, $\bar{\gamma}_{12}^{\text{EB}}$, and $\bar{\gamma}_{22}^{\text{EB}}$ of state σ_{AB} from bounds on $\bar{\gamma}_{11}, \bar{\gamma}_{12}$ and $\bar{\gamma}_{22}$. Then invoke the Gaussian extremality theorem to state that the Holevo information $\chi(B;E)_{\overline{\mathcal{U}}(\theta(N_S))}$ is maximized by a Gaussian state with the covariance matrix given in (210). By combining the upper bound obtained on $\chi(B;E)_{\overline{\mathcal{U}}(\theta(N_S))}$ with (164), we obtain an upper bound on $\chi(B;E)_{\mathcal{U}(\overline{\rho})}$.

The method outlined above does succeed in obtaining a security proof for discrete-modulation protocols with no dependence on the parameters c_1 and c_2. However, as of now it seems that this method is numerically intensive.