Security of continuous-variable quantum key distribution against canonical attacks

Panagiotis Papanastasiou
Computer Science
University of York
York, United Kingdom
panagiotis.papanastasiou@york.ac.uk

Carlo Ottaviani
Computer Science
University of York
York, United Kingdom
carlo.ottaviani@york.ac.uk

Stefano Pirandola
Computer Science
University of York
York, United Kingdom
stefano.pirandola@york.ac.uk

Abstract—We investigate the performance of Gaussian-modulated coherent-state QKD protocols in the presence of canonical attacks, which are collective Gaussian attacks resulting in Gaussian channels described by one of the possible canonical forms. We present asymptotic key rates and then we extend the results to the finite-size regime using a recently-developed toolbox for composable security.

Index Terms—Continuous variables, quantum key distribution, Gaussian modulation, finite-size effects, composable security

I. INTRODUCTION

A quantum key distribution (QKD) protocol describes the communication steps performed by two remote authenticated parties to establish a shared key even though the link between them is potentially compromised [1]. The information-theoretic security of such a protocol is granted by the laws of nature (quantum mechanics) [2], [3]. The first protocols designed were based on discrete variable (DV) systems, while more recently proposed protocols use continuous variables (CV), i.e., the position and momentum quadratures of the bosonic modes of the electromagnetic field [4], [5]. In particular, CV-QKD protocols using Gaussian modulation of coherent states for the encoding of information [6]–[8] can be easily implemented using the current telecommunication infrastructure and may achieve high rates close to the PLOB bound for repeaterless quantum communications in a lossy channel [9]. More specifically, these protocols can be considered as coming from a single scheme with different aspects [5]: reverse reconciliation (RR) or direct reconciliation (DR), with homodyne or heterodyne decoding measurement.

Their security analysis was first studied for asymptotic key rates under the assumption of collective Gaussian attacks [10], [11], completely characterized by Ref. [12]. Later, security was extended to the finite size regime [13]–[15] and to a general composable framework [16], [17], including free-space [17] and satellite-based scenarios [18]. Proof-of-principle and in-field experiments have been recently demonstrated in long ground-based fiber connections [19]–[21]. As pointed out in Ref. [12], single-mode Gaussian channels and the corresponding collective Gaussian attacks can be classified in different canonical forms. One of these forms is represented by the thermal-loss (attenuation) channel and the associated collective entangling-cloner attack, typically assumed in CV-QKD security proofs.

Here we present the asymptotic secret key rates of the Gaussian-modulated coherent-state protocols with respect to the other canonical forms. Besides the attenuation channel, these include the amplifying channel, the additive classical-noise channel and other more exotic Gaussian channels [5], [12]. Then, using the toolbox of Ref. [17] for composable security under general channel conditions, we extend the analysis of the amplifying and classical-noise channels to include finite-size effects and composable security.

After a short description of the canonical forms in Sec. II, in Sec. III we describe the security analysis in the asymptotic regime in the presence of a generic canonical form for the cases of for homodyne or heterodyne protocol in RR/DR. In Sec. IV, we present the results of the previous analysis specified for each canonical form by assuming ideal reconciliation efficiency and large modulation. In Sec. V, we perform the parameter estimation (PE) following Refs. [14], [15] and in Sec. VI we compute the composable key rates using Ref. [17].

II. CANONICAL FORMS

Recall that a Gaussian channel $\mathcal{G}(\mathbf{T}, \mathbf{N}, \mathbf{d})$ acting on a single mode, for $\mathbf{T}, \mathbf{N}$ 2×2 real matrices and $\mathbf{d}$ an $\mathbb{R}^2$ vector, is a completely positive trace-preserving map that maintains the Gaussian statistics of the input state. It can be mapped to its canonical form $\mathcal{C}$, which is a Gaussian channel with $\mathbf{d} = 0$ and $\mathbf{T}_c$, $\mathbf{N}_c$ diagonal, by $\mathcal{G} = \mathcal{U}_A \circ \mathcal{C} \circ \mathcal{U}_B$, where $\mathcal{U}_A$ and $\mathcal{U}_B$ are Gaussian unitaries. One can reduce the description of $\mathbf{T}_c$, $\mathbf{N}_c$ to three symplectic invariants: the generalized transmission $\tau = \det \mathbf{T}$, for $-\infty < \tau < \infty$, the rank $r = (\text{rk}(\mathbf{T})\text{rk}(\mathbf{N}))/2$ for $r = 0, 1, 2$ and the temperature $\bar{n}$, connected to $\det \mathbf{N}$.

According to the first two parameters, the canonical forms can be grouped into different classes: The class A_1 for $\tau = 0$, $r = 0$, which replaces the input states with thermal states (completely depolarizing channel). The classes A_2 and B_1 for $\tau = 0$, $r = 1$ and $\tau = 1$, $r = 1$ transforming the quadratures asymetrically. B_2 is the additive classical-noise channel for $\tau = 1$ and $r = 2$ and it collapses to the identity channel for $\bar{n} = 0$. Class C is connected to channels

with transmissivity, i.e., $0 < \tau \neq 1$ and $r = 2$, with the subcases $\tau < 1$ (attenuation channel) and $\tau > 1$ (amplifying channel). Finally, the class D, where its output can be seen as complementary to the amplifying channel and is connected to negative transmissivities.

Via the Stinespring dilation, one can represent the canonical form $\mathcal{C}(\tau, r, \bar{n})$ with a unitary symplectic transformation $\mathcal{L}(\tau, r)$ mixing the input state and a two-mode squeezed-vacuum (TMSV) state with variance $\omega = 2\bar{n} + 1$, which describes the environment. In more detail, apart from the class B_2, we have that $\mathcal{L}(\tau, r) = \mathcal{M}(\tau, r) \oplus \mathbf{I}$ where $\mathcal{M}(\tau, r)$ is a symplectic form interacting only with the input state and one mode from the TMSV state, with the other mode being subject to the identity $\mathbf{I}$. For the class B_2, we adopt a description using the attenuation channel as we will see later.

The unitary dilation of the canonical form represents the Gaussian interaction performed by the eavesdropper that controls the TMSV state of the environment [12]. After interaction with the input mode, the environmental output is stored in a quantum memory, that will be subject to a joint and optimal measurement (collective attack).

III. ASPECTS OF THE PROTOCOL SCHEME

Alice picks randomly $2N$ samples $\{x_i\}$ from the variable x distributed according to the normal distribution

$$p(x) = (\sqrt{2\pi V_A})^{-1} \exp\left[-x^2/(2V_A)\right] \quad (1)$$

with zero mean and variance V_A. Then she modulates mode A carrying coherent states $|\alpha\rangle$ according to these samples with

$$\alpha = (q_A + ip_A)/2 = (x_{2j-1} + ix_{2j})/2, \quad (2)$$

where q_A and p_A are the encoding on the quadratures and $j = 1, \ldots, N$. In the asymptotic regime ($N \gg 1$), the covariance matrix (CM) of Alice's ensemble state is given by $\mathbf{V}_A = \mu\mathbf{I}$ with $\mathbf{I} = \text{diag}\{1,1\}$ and $\mu = V_A + 1$. Mode A is traveling through a quantum channel modeled by one of the canonical forms [5], [12]. In particular, Eve's system is described by two modes E and e in a TMSV state with variance ω and covariance matrix

$$\mathbf{V}_{Ee} = \begin{pmatrix} \omega\mathbf{I} & \sqrt{\omega^2 - 1}\mathbf{Z} \\ \sqrt{\omega^2 - 1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix}, \quad (3)$$

where $\mathbf{Z} = \text{diag}\{1, -1\}$. Mode E is mixed with A via a canonical form whose dilation is represented by a symplectic matrix $\mathcal{M}$ (e.g., this is a beam-splitter transformation in the case of an attenuation channel). One output mode B goes to Bob, while the other E' goes to Eve. Eve's idler mode e and mode E' are kept in a quantum memory for a later optimal measurement. Then the CM for modes B, E', and e is given by

$$\mathbf{V}_{BE'e} = (\mathcal{M}^\mathsf{T} \oplus \mathbf{I})(\mathbf{V}_A \oplus \mathbf{V}_{Ee})(\mathcal{M} \oplus \mathbf{I}), \quad (4)$$

which can be expressed as follows

$$\mathbf{V}_{BE'e} = \begin{pmatrix} \mathbf{V}_B & \mathbf{C}_{BE'} & \mathbf{C}_{Be} \\ \mathbf{C}_{BE'} & \mathbf{V}_{E'} & \mathbf{C}_{E'e} \\ \mathbf{C}_{Be} & \mathbf{C}_{E'e} & \mathbf{V}_e \end{pmatrix}. \quad (5)$$

From the previous CM, we can derive the CM of Eve's average state by tracing out mode B and Bob's CM by tracing out $E'e$ respectively. Therefore, we obtain

$$\mathbf{V}_{E'e} = \begin{pmatrix} \mathbf{V}_{E'} & \mathbf{C}_{E'e} \\ \mathbf{C}_{E'e} & \mathbf{V}_e \end{pmatrix}, \quad \mathbf{V}_B = \text{diag}\{V_B^q(V_A), V_B^p(V_A)\} \quad (6)$$

where $\mathbf{V}_{E'} = \text{diag}\{V_{E'}^q(V_A), V_{E'}^p(V_A)\}$ is a function of V_A. In general, the canonical forms may treat the quadratures q and p asymmetrically resulting in different variances V_B^q and V_B^p or V_E^q and V_E^p respectively. Note that for the class C and the classical-noise channel the treatment is symmetric so we have $V_B^q = V_B^p = V_B$ and $V_{E'}^q = V_{E'}^p = V_{E'}$.

In the homodyne protocol, Bob measures either the q-quadrature or p-quadrature of the arriving mode with outcome q_B or p_B respectively. He informs Alice about the choice of quadrature and then she keeps only the relevant encoding q_A or p_A respectively (shifting the outcomes). In contrast, in the heterodyne protocol, Bob measures both quadratures and Alice's encoding is described by the pair q_A, p_A and Bob's outcome by q_B, p_B.

For the homodyne protocol in DR, we derive Eve's conditional CM $\mathbf{V}_{E'e|q_A}$ (respectively $\mathbf{V}_{E'e|p_A}$) on Alice's encoding q_A (or p_A) given by (6) up to the replacement of $\mathbf{V}_{E'}$ with $\text{diag}\{V_{E'}^q(0), V_{E'}^p(V_A)\}$ (respectively with $\text{diag}\{V_{E'}^q(V_A), V_{E'}^p(0)\}$); for the heterodyne protocol, the conditional CM $\mathbf{V}_{E'e|q_A,p_A}$ is given by replacing $\mathbf{V}_{E'}$ by $\text{diag}\{V_{E'}^q(0), V_{E'}^p(0)\}$ in the same equation.

Let us now compute Eve's conditional CM on Bob's measurement outcome l_B, with l equal to either q or p for a different quadrature, in RR. For the homodyne protocol, we obtain [5]

$$\mathbf{V}_{E'e|l_B} = \mathbf{V}_{E'e} - \mathbf{C}_{BE'e}^\mathsf{T}(\Pi_l \mathbf{V}_B \Pi_l)^{-1}\mathbf{C}_{BE'e}, \quad (7)$$

where $\mathbf{C}_{BE'e} = \begin{pmatrix} \mathbf{C}_{BE'} \\ \mathbf{C}_{Be} \end{pmatrix}$, $\Pi_q = \text{diag}\{1, 0\}$, $\Pi_p = \text{diag}\{0, 1\}$, and $(.)^{-1}$ corresponds here to the calculation of the pseudo-inverse. If Bob's measurement is a heterodyne measurement then the conditional CM is given by [5]

$$\mathbf{V}_{E'e|q_B,p_B} = \mathbf{V}_{E'e} - \mathbf{C}_{BE'e}^\mathsf{T}(\mathbf{V}_B + \mathbf{I})^{-1}\mathbf{C}_{BE'e}. \quad (8)$$

Let us assume now a very large number of exchanged signals ($N \gg 1$). Then the mutual information between the encoding q_A or p_A and the outcome q_B or p_B for the homodyne protocol is given by

$$I(\mu, \tau, \omega) = \frac{1}{2}\left(\frac{1}{2}\log_2 \frac{V_B^q}{V_{B|q_A}^q} + \frac{1}{2}\log_2 \frac{V_B^p}{V_{B|p_A}^p}\right), \quad (9)$$

for $V_{B|l_A}^l = V_B^l(0)$, where we have assumed that half of the times Bob's outcome is q_B and otherwise p_B. On the other hand, the mutual information between the encoding q_A, p_A and the outcome q_B, p_B for the heterodyne protocol is given by

$$I(\mu, \tau, \omega) = \frac{1}{2}\left(\log_2 \frac{V_B^q + 1}{V_{B|q_A}^q + 1} + \log_2 \frac{V_B^p + 1}{V_{B|p_A}^p + 1}\right). \quad (10)$$

Eve's Holevo information is calculated by the symplectic spectrum $\boldsymbol{\nu}_{E'e}$ of the CM $\mathbf{V}_{E'e}$ and the spectra, $\boldsymbol{\nu}_{E'e|q_A}$, $\boldsymbol{\nu}_{E'e|p_A}$ and $\boldsymbol{\nu}_{E'e|q_A,p_A}$ or $\boldsymbol{\nu}_{E'e|q_B}$, $\boldsymbol{\nu}_{E'e|p_B}$ and $\boldsymbol{\nu}_{E'e|q_B,p_B}$, associated with the conditional CMs in DR or RR respectively. More specifically, for the homodyne protocol, we have that

$$
\chi(\mu,\tau,\omega) = \sum_{i=1,2} h\left([\boldsymbol{\nu}_{E'e}]_i\right)
$$
$$
- \frac{1}{2}\left(\sum_{i=1,2} h\left([\boldsymbol{\nu}_{E'e|q_\gamma}]_i\right) + \sum_{i=1,2} h\left([\boldsymbol{\nu}_{E'e|p_\gamma}]_i\right)\right), \tag{11}
$$

while for the heterodyne protocol

$$
\chi(\mu,\tau,\omega) = \sum_{i=1,2} h\left([\boldsymbol{\nu}_{E'e}]_i\right) - \sum_{i=1,2} h\left([\boldsymbol{\nu}_{E'e|q_\gamma,p_\gamma}]_i\right),
$$

where

$$
h(x) = \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}, \tag{12}
$$

with γ being either A or B for the protocol in DR or RR respectively, Then the asymptotic secret key rate is obtained by [1]

$$
R(\mu,\tau,\omega) = \zeta I(\mu,\tau,\omega) - \chi(\mu,\tau,\omega), \tag{13}
$$

where ζ is the reconciliation efficiency parameter.

IV. ASYMPTOTIC KEY RATES

Here we calculate the asymptotic secret key rate for each of the canonical forms assuming an ideal reconciliation efficiency $\zeta = 1$ and the large modulation limit $\mu \to \infty$. In fact, we present results in detail for the practical cases of attenuation, amplifying, and classical-noise channel. Class B_1 is always secure (see Appendix for more details) while classes D and A_2 do not provide a secret key rate, i.e., for any set of parameters describing the corresponding canonical form the parties cannot extract a secret key. The whole class of such channels have the property of anti-degradability [5]: In terms of cryptography, the eavesdropper (Eve) can obtain the receiver's (Bob's) state by applying a CPT map on the state of the environment forbidding the secret key extraction. However, for classes with members that may hold this property or not, e.g., the attenuation channel for $\tau < 1/2$ against the cases with $\tau \geq 1/2$, the RR can provide a remedy.

A. C class

The symplectic matrix associated with the dilation of the C class is

$$
\mathcal{M}_{\text{Att}}(0 < \tau < 1) = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix} \tag{14}
$$

and

$$
\mathcal{M}_{\text{Amp}}(\tau > 1) = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{\tau-1}\mathbf{Z} \\ \sqrt{\tau-1}\mathbf{Z} & \sqrt{\tau}\mathbf{I} \end{pmatrix} \tag{15}
$$

for the attenuation and amplifying channel respectively. Following the steps in Sec. III, one easily obtains the secret key
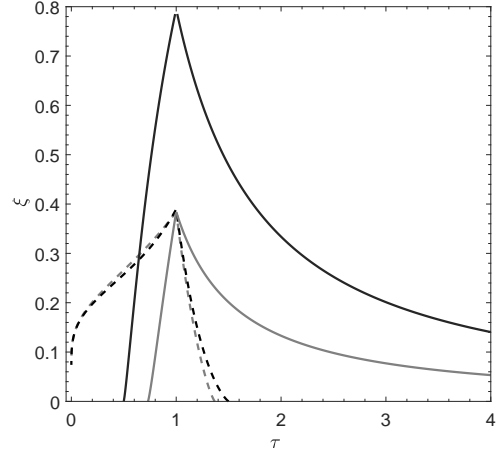

Fig. 1. The asymptotic security thresholds of the C class for transmisivities $\tau > 0$ ($\tau \neq 1$) with respect to the excess noise ξ, where the reconciliation has been considered ideal and $\mu \to \infty$. We plot the homodyne protocol in DR (black solid line) and in RR (black dashed line) and the heterodyne protocol in DR (gray solid line) and in RR (gray dashed line). The instances with high excess noise (above the threshold lines) give no secret key rate.

rates for the homodyne (hom) and heterodyne (het) protocols in DR (▶) and RR (◀). We have

$$
R_{\text{hom}}^{\blacktriangleright}(\tau,\omega) = \frac{1}{2}\log_2\frac{\tau(\tau\omega + |1-\tau|)}{|1-\tau|(\tau + |1-\tau|\omega)}
$$
$$
- h(\omega) + h\left(\sqrt{\frac{\omega(\tau + |1-\tau|\omega)}{|1-\tau| + \tau\omega}}\right), \tag{16}
$$

$$
R_{\text{hom}}^{\blacktriangleleft}(\tau,\omega) = \frac{1}{2}\log_2\frac{\omega}{|1-\tau|(\tau + (|1-\tau|)\omega)} - h(\omega), \tag{17}
$$

$$
R_{\text{het}}^{\blacktriangleright}(\tau,\omega) = \log_2\frac{2\tau}{e|1-\tau|(\tau + |1-\tau|\omega + 1)}
$$
$$
- h(\omega) + h(\tau + |1-\tau|\omega), \tag{18}
$$

$$
R_{\text{het}}^{\blacktriangleleft}(\tau,\omega) = \log_2\frac{2\tau}{e|1-\tau|(\tau + |1-\tau|\omega + 1)}
$$
$$
- h(\omega) + h\left(\frac{1 + |1-\tau|\omega}{\tau}\right). \tag{19}
$$

In Fig. 1, we plot the security threshold for each of the cases above with respect to transmissivity and excess noise $\xi = \frac{|1-\tau|(\omega-1)}{\tau}$. Then, in Fig. 2, for $\omega := 1$ (no thermal noise), $\zeta = 1$, and $\tau := 10^{\frac{-L}{10}}$ where L is the attenuation in dB, we plot (16), (18), (17) and (19). In Fig. 3, we plot the same cases for $\tau := 10^{\frac{L}{10}}$ with L being the gain in dB.

B. Classical-noise channel

To simulate a Gaussian channel with additive classical-noise, we adopt the symplectic matrix of a beam splitter

$$
\mathcal{M}_{\text{Att}}(0 < \tau < 1) = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix} \tag{20}
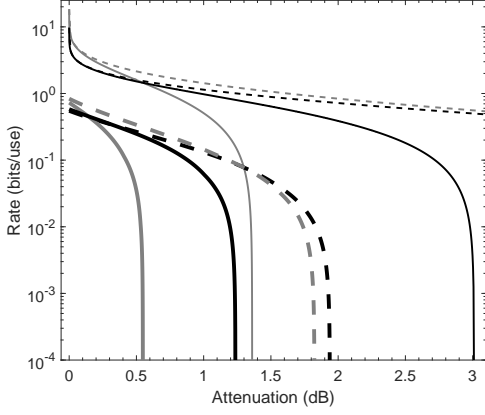$$

Fig. 2. Secret key rate versus attenuation in dB for an attenuation channel. With thin lines, we plot the asymptotic rate for the homodyne protocol in DR (black solid) and in RR (black dashed) and for the heterodyne protocol in DR (gray solid) and in RR (gray dashed) for $\xi = 0$, $\zeta = 1$, and $\mu \to \infty$. For the composable secret key rates (corresponding thick lines), we have assumed channel excess noise $\xi = 0.01$ and conservative values for the parameters $\zeta = 0.9$, $p_{EC} = 0.8$, and $N = 10^6$. We have optimized over the ratio r and the modulation V_A with $\epsilon_{PE} \approx 10^{-10}$, $\epsilon_s = \epsilon_h = 10^{-20}$, and $d = 2^5$. The plots of the asymptotic key rate evaluate the security of the protocol and the associated performance taking into account only theoretical aspects, e.g. the kind of attack, focusing more on the quantum communication part of the protocol. On the contrary, the finite-size analysis in a composable framework takes also into account the classical post-processing parts of the protocol providing with a performance close to a practical implementation usually expected to be worse than the ideal case as it is supported by the plots in thick lines compared with the corresponding cases in thin lines. We observe here that the heterodyne protocols behave better in closer distances (higher signal to noise ratio) compared with the homodyne protocols since they can take into advantage the double encoding into the same signal. Despite this fact, the homodyne protocols have achievable rates in longer distances. In fact, they behave better against the excess noise in long distances and, in particular the RR protocol, against the parameter estimation effects connected to the excess noise and transmissivity.

and take the joint limits for $\tau \to 1$ and $\omega \to \infty$ so that $(1 - \tau)\omega = \theta$, for some constant variance θ of the additive noise. The corresponding secret key rates are given by

$$R_{\text{hom}}^{\blacktriangleright}(\theta) = \log_2\left(\frac{2}{e\sqrt{\theta(\theta+1)}}\right) + h(\sqrt{1+\theta}), \quad (21)$$

$$R_{\text{hom}}^{\blacktriangleleft}(\theta) = \log_2\left(\frac{2}{e\sqrt{\theta(\theta+1)}}\right), \quad (22)$$

$$R_{\text{het}}^{\blacktriangleright}(\theta) = R_{\text{het}}^{\blacktriangleleft}(\theta) = \log_2\left(\frac{4}{e^2\theta(\theta+2)}\right) + h(\theta+1), \quad (23)$$

We plot (21), (22) and (23) in Fig. 4.

V. PARAMETER ESTIMATION

A. Attenuation channel

Let us assume a protocol with homodyne detection. Here Bob's measurement outcome is described by the generic variable
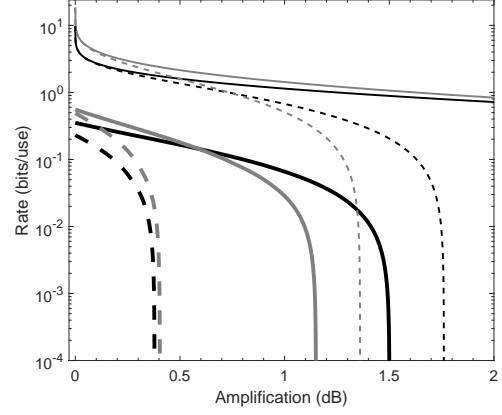
$$y = \sqrt{\tau}x + z \quad (24)$$

Fig. 3. Asymptotic key rates in the presence of an amplifying channel. With thin lines, we plot the asymptotic rate for the homodyne protocol in DR (black solid) and in RR (black dashed) and for the heterodyne protocol in DR (gray solid) and in RR (gray dashed) for $\xi = 0$, $\zeta = 1$ and $\mu \to \infty$. For the composable secret key rates (corresponding thick lines), we have assumed channel excess noise $\xi = 0.01$ and conservative values for the parameters $\zeta = 0.9$, $p_{EC} = 0.8$, and $N = 10^6$. We have optimized over the ratio r and the modulation V_A with $\epsilon_{PE} \approx 10^{-10}$, $\epsilon_s = \epsilon_h = 10^{-20}$, and $d = 2^5$. Here we observe that the RR and DR protocols have the opposite behaviour compared with the attenuation channel case, i.e., we have smaller achievable rate distances for the RR protocols instead for the DR protocols. Comparing also the composable rates of the RR protocols, it seems that in the regime of $N = 10^6$, the homodyne protocol cannot surpass the performance of the heterodyne protocol due to the fact that the gain variance plays an important role in the amplifying channel: the coefficient in front of the gain variance in (32) is double its counterpart in (33).

where y describes either the outcome connected with the quadrature q or p. Accordingly, the variable x describes Alice's encoding while

$$z = \sqrt{\tau}x_s + \sqrt{1-\tau}x_o + x_\Xi, \quad (25)$$

is a variable representing the noise detected by Bob. The variables x_s and x_o have equal variance $V_s = V_o = 1$ describing the quantum shot noise, and the variable x_Ξ with variance $\Xi := \tau\xi$ describes the excess noise of the channel $\xi = \frac{(1-\tau)(\omega-1)}{\tau}$. Therefore we obtain the noise variance

$$\sigma_z^2 = \Xi + 1. \quad (26)$$

Based on the previous analysis and assuming m signals for PE, we derive the variances of the maximum likelihood estimators (MLEs) $\hat{\tau}$ and $\hat{\Xi}$ of the transmissivity and excess noise according to Ref. [15]. Therefore, the worst case scenario values for the channel parameters are given by

$$\tau_m = \tau - w\sigma_\tau, \quad \Xi_m = \Xi + w\sigma_\Xi, \quad (27)$$

with $w = \sqrt{2}\text{erf}^{-1}(1 - \epsilon_{PE})$, as the extremal values of the intervals defined by the estimator variances

$$\sigma_\tau^2 = \frac{4\tau^2}{m}\left(2 + \frac{\sigma_z^2}{\tau V_A}\right), \quad \sigma_\Xi^2 = 2\frac{\sigma_z^4}{m}, \quad (28)$$

where $\text{erf}(.)$ is the error function and ϵ_{PE} is the associated error probability.
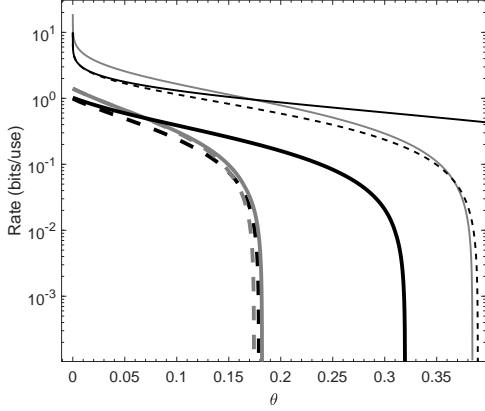
Fig. 4. Secret key rate for a classical-noise channel against the classical thermal noise θ. With thin lines, we plot the asymptotic rate for the homodyne protocol in DR (black solid) and in RR (black dashed) and for the heterodyne protocol in DR (gray solid) and in RR (gray dashed) for $\xi = 0$, $\zeta = 1$ and $\mu \to \infty$. Note that the lines for the heterodyne protocol in DR and RR coincide. For the composable secret key rates (corresponding thick lines), we have assumed channel excess noise $\xi = 0.01$ and conservative values for the parameters $\zeta = 0.9$, $p_{EC} = 0.8$, and $N = 10^6$. We have optimized over the ratio r and the modulation V_A with $\epsilon_{PE} \approx 10^{-10}$, $\epsilon_s = \epsilon_h = 10^{-20}$, and $d = 2^5$. Here we observe that the most robust protocol against classical thermal noise is the homodyne protocol in DR while the other cases have similar performance.

In the heterodyne protocol, Bob mixes the incoming mode B with a vacuum mode in a balanced beam splitter. Then he applies two conjugate homodyne detections to the beam-splitter outputs. Due to the presence of the extra vacuum mode, the outputs have an increased noise variance by 1 shot noise units compared with the protocol using homodyne measurement. In addition, there is an estimator for τ and Ξ from each one of the quadratures. These are optimally combined and give the variances

$$\sigma_\tau^2 = \frac{2\tau^2}{m}\left(2 + \frac{\sigma_z^2 + 1}{\tau V_A}\right) \text{ and } \sigma_\Xi^2 = \frac{(\sigma_z^2 + 1)^2}{m}. \quad (29)$$

Finally, the key rate in Eq. (13) is expressed via the parameter Ξ as $\tilde{R}(\mu, \tau, \Xi) = R(\mu, \tau, \omega)$ and by setting the worst case scenario values one obtains the secret key rate after PE

$$R_m = \tilde{R}(\mu, \tau_m, \Xi_m). \quad (30)$$

B. Amplifying channel

Here, Bob detects noise described by the variable

$$z = \sqrt{\tau}x_s \pm \sqrt{\tau - 1}x_o + x_\Xi \text{ with } \sigma_z^2 = 2\tau + \Xi - 1 \quad (31)$$

where $\Xi := \tau\xi$, $\xi = \frac{(\tau-1)(\omega-1)}{\tau}$ resulting in estimator variances

$$\sigma_\tau^2 = \frac{4\tau^2}{m}\left(2 + \sigma_z^2/(\tau V_A)\right), \quad \sigma_\Xi^2 = 2\frac{\sigma_z^4}{m} + 4\sigma_\tau^2 \quad (32)$$

for the homodyne protocol and

$$\sigma_\tau^2 = \frac{2\tau^2}{m}\left(2 + (\sigma_z^2 + 1)/(\tau V_A)\right), \quad \sigma_\Xi^2 = \frac{(\sigma_z^2 + 1)^2}{m} + 2\sigma_\tau^2 \quad (33)$$

for the heterodyne protocol. Finally, one calculates the corresponding secret key rate R_m after PE as in (30).

C. Classical-noise channel

For the classical-noise channel we adopt the same analysis as in Sec. V-A in addition to the assumption of

$$\Xi = \tau\xi = (1 - \tau)\omega - (1 - \tau) \text{ with } \lim_{\tau \to 1}\Xi = \theta. \quad (34)$$

This leads to the following relations for the noise variance

$$\sigma_z^2 = \theta + 1, \quad (35)$$

Therefore we obtain the worst case estimator

$$\Xi_m = \Xi + w\sigma_\Xi \text{ with } \sigma_\Xi^2 = 2\frac{\sigma_z^4}{m} \quad (36)$$

for the homodyne protocol and $\sigma_\Xi^2 = \frac{(\sigma_z^2 + 1)^2}{m}$ for the heterodyne protocol. Then one obtains the corresponding secret key rate R_m after PE as in (30).

VI. COMPOSABLE KEY RATES

According to Ref. [17], the composable key rate takes the form

$$R \geq r\left[R_m - n^{-1/2}\Delta_{AEP} + n^{-1}\Theta\right], \quad (37)$$

where

$$\Theta := \left\{\log_2[p\left(1 - \epsilon_s^2/3\right)] + 2\log_2\sqrt{2}\epsilon_h\right\}, \quad r = \frac{np_{EC}}{N} \quad (38)$$

and

$$\Delta_{AEP} := 4\log_2\left(2\sqrt{d} + 1\right)\sqrt{\log(18/(p^2\epsilon_s^4))}, \quad (39)$$

is the correction term for using the von Neumann entropy in the calculation of a finite-size rate and is dependent on the number of bins d used during the discretization step of the variables. The frame error rate $1 - p_{EC}$ is the number of blocks with initial size N that passed through the error correction (EC) step while $n = N - m$ is the portion of signals devoted to secret key creation. With ϵ_s, ϵ_h, ϵ_{PE}, and ϵ_{cor} we denote the smoothing parameter, the privacy amplification (hashing) parameter, the channel estimation parameter, and the EC parameter. Note that p_{EC} is a function of ϵ_{EC} but their relation can only be evident in a specific practical implementation of the protocol. Each ϵ parameter quantifies a distance from an ideal implementation of each step of the protocol. An overall security parameter can then be calculated by composing these parameters into a sum $\epsilon = \epsilon_S + \epsilon_{cor} + \epsilon_h + 2p_{EC}\epsilon_{PE}$.

In Figs. 2, 3, and 4, we present results regarding the secret key rate in the composable framework for the attenuation, amplifying, and additive classical thermal noise channel, respectively. We assume conservative values for the parameters $N = 10^6$, $\beta = 0.9$, and $p_{EC} = 0.8$ due to limitations that may occur in the data post-processing procedure [22]. However, still, the protocols provide the parties with positive rates at metropolitan distances, e.g., ≈ 10 km [see Fig. 2 (black thick dashed line)]. The security parameters have been set to $\epsilon_{PE} \approx 10^{-10}$ and $\epsilon_s = \epsilon_h = 10^{-20}$. In addition, we chose $d = 2^5$ and we optimized over r and V_A.

VII. CONCLUSION

In this work we expanded the security of CV-QKD to all canonical forms. We studied first the asymptotic security, then we focused on the finite-size and composable security. We first provided a compact description of the asymptotic secret-key rates of practical channels like the attenuation, amplification, and the classical-noise channels. Then our analysis discussed in more detail the impact of parameter estimation and that of other finite-size effects on the secret-key rates achievable over these channels. We also computed the secret-key rate for more exotic Gaussian channels finding that we either obtain an always positive key rate (for B_1 assuming large Gaussian modulation) or no asymptotic secret key rate (for the forms D and A_2). This analysis can be expanded, in future works, to protocols that use squeezed and/or thermal states, protocols with discrete alphabets, or CV measurement device independent schemes, in each case by assuming links described by the previous channel classes.

ACKNOWLEDGMENTS

REFERENCES

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).

[2] J. Park, "The concept of transition in quantum mechanics", Foundations of Physics **1**, 23–33 (1970).

[3] W. Wootters, and W. Zurek, "A single quantum cannot be cloned", Nature **299**, 802 (1982).

[4] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables", Rev. Mod. Phys. **77**, 513 (2005).

[5] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information", Rev. Mod. Phys. **84**, 621 (2012).

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

[7] F. Grosshans, G. Van Assche, and J. Wenger, et al., "Quantum key distribution using gaussian-modulated coherent states", Nature **421**, 238 (2003).

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

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

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

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

[12] S. Pirandola, S. L. Braunstein, and S. Lloyd, "Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography", Phys. Rev. Lett. **101**, 200504 (2008).

[13] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution", Phys. Rev. A **81**, 062343 (2010).

[14] L. Ruppert, V. C. Usenko, and R. Filip, "Long-distance continuous-variable quantum key distribution with efficient channel estimation", Phys. Rev. A **90**, 062310 (2014).

[15] P. Papanastasiou, C. Ottaviani, and S. Pirandola, "Gaussian one-way thermal quantum cryptography with finite-size effects", Phys. Rev. A **98**, 032314 (2018).

[16] A. Leverrier, "Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction," Phys. Rev. Lett. **118**, 200501 (2017).

[17] S. Pirandola, "Limits and Security of Free-Space Quantum Communications", Physical Review Research **3**, 013279 (2021).

[18] S. Pirandola, "Satellite Quantum Communications: Fundamental Bounds and Practical Security", arXiv:2012.01725 (2020).

[19] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network", Opt. Lett. **41**, 3511 (2016).

[20] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang et al., "Continuous-variable QKD over 50 km commercial fiber", Quantum Sci. Technol. 4, 035006 (2019).

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

[22] A. G. Mountogiannakis, P. Papanastasiou, B. Braverman, and S. Pirandola, "Composably secure data processing in continuous-variable quantum key distribution", arXiv:2103.16589 (2021).

APPENDIX

The asymptotic secret key rates for the canonical form B_1 associated with the symplectic transformation

$$\mathcal{M}_{B_1} = \begin{pmatrix} \mathbf{I} & \frac{\mathbf{I}+\mathbf{Z}}{2} \\ \frac{\mathbf{I}-\mathbf{Z}}{2} & -\mathbf{I} \end{pmatrix} \tag{40}$$

are given by

$$R_{\text{hom}}^{\blacktriangleright}(\mu) = \frac{1}{2} \log_2 \frac{\sqrt{2\mu}}{e} + \frac{1}{2} h(\sqrt{2}), \tag{41}$$

$$R_{\text{hom}}^{\blacktriangleleft}(\mu) = \frac{1}{2} \log_2 \frac{\sqrt{2\mu}}{e}, \tag{42}$$

$$R_{\text{het}}^{\blacktriangleright}(\mu) = R_{\text{het}}^{\blacktriangleleft}(\mu) = \log_2 \frac{\sqrt{2\mu}}{e\sqrt{3}} + h(\sqrt{2}). \tag{43}$$