Lower bounding the secret key capacity of bosonic Gaussian channels via optimal Gaussian measurements

Giuseppe Ortolano [1,2], Stefano Pirandola [3] and Leonardo Banchi [1,2]

[1] *Dipartimento di Fisica e Astronomia, Università di Firenze, Via G. Sansone 1, I-50019 Sesto Fiorentino (FI), Italy*

[2] *Istituto Nazionale di Fisica Nucleare, Sezione di Firenze, via G. Sansone 1, I-50019 Sesto Fiorentino (FI), Italy*

[3] *Department of Computer Science, University of York, York YO10 5GH, United Kingdom*

(Received 12 February 2026; revised 8 June 2026; accepted 2 October 2026; published 28 October 2026)

We find the maximum rate achievable in the private communication over a bosonic quantum channel with a fully Gaussian protocol based on optimal single-mode Gaussian measurements. This rate establishes a lower bound on the secret rate capacity of the channel. We focus on the class of phase-insensitive Gaussian channels. For the thermal loss and thermal amplification channels, our results demonstrate the optimality, within the constraints of our analysis, of previously proposed protocols, while also providing a significantly simplified formula for their performance evaluation. For the added noise channel, our rate provides a better lower bound than any previously known.

DOI: 10.1103/v53z-9gtm

I. INTRODUCTION

Quantum key distribution (QKD) [1–6] is a central pillar of quantum information, aimed at establishing provably secure communication. A central task in QKD is to find the secret rate capacity, the rate at which two parties can generate a shared private key, by communicating over a quantum channel. This task is particularly relevant for bosonic quantum channels, which model a wide range of physical interactions in continuous variable (CV) quantum communication [7–9]. Among these, Gaussian quantum channels are especially important, as they model practical systems, such as optical fibers and free-space communication.

In this context, Ref. [10] established a general upper bound on the secret rate capacity. For the specific case of pure-loss channels, this bound matches the previously known lower bound [11], yielding an exact, closed-form expression for the capacity. On the other hand, the capacity for the similarly important thermal loss, thermal amplification, and added noise channels, remains unknown, with separate upper and lower bounds. For these channels, the use of coherent [12,13] and reverse coherent [11,14] information, together with the relative entropy of entanglement [15–17] fails to close the gap.

In the present work, we further the effort in closing the gap between bounds for the aforementioned phase-insensitive channels by providing a lower bound via the computation of the maximum secret rate achievable by a fully Gaussian protocol operating optimized single-mode Gaussian measurements. Our work confirms previous results for the thermal loss and thermal amplification channels, while providing a tighter lower bound for the added-noise channel.

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

The paper is structured as follows. In Sec. I, we define the secret rate capacity in the context of our protocol. In Sec. II, we characterize the capacity for a fully Gaussian protocol, and we present the results for phase-insensitive channels. In Sec. III, we summarize the conclusions of our work.

II. SECRET KEY RATE

Consider a communication scheme in the entanglement-based representation that involves two parties, Alice and Bob, as depicted in Fig. 1. Alice retains one system (A) of a two-mode squeezed vacuum (TMSV) state, Φ_{AB}, with parameter $\mu = 2\bar{n} + 1$, where $\bar{n}$ is the mean number of photons in each marginal state. In the following we will consider all the relevant quantities in the limit of $\mu \to \infty$. The other system (B) is sent to Bob via a Gaussian channel $\mathcal{E}$, with parameters η (transmissivity or gain) and ω (thermal-noise variance) [11]. Communication is achieved by performing a local, single-mode POVM $\Pi_X = \{\Pi_x\}$ either on A (direct reconciliation) or B (reverse reconciliation). Let us denote in the following the party that performs the encoding measurement as the sender $X = A/B$ and the other party as $Y = B/A$. The rate of communication of this scheme, R_{XY} is upper bounded by the χ quantity:

$$R_{XY} \leqslant \chi_Y^{\Pi_X} := S(\rho_Y) - \sum_x p_x S(\rho_{Y|x}), \tag{1}$$

where p_x is the probability of outcome x, $X = A, Y = B (X = B, Y = A)$ in direct (reverse) reconciliation and ρ_Y is the total local state of Y and $\rho_{Y|x}$ is the conditioned state of Y to outcome x on system X. In the limit of many uses of the channel and unlimited one-way classical communication the right-hand side of Eq. (1) is exactly the common randomness between parties X and Y distillable from the classical-quantum system, resulting from the measurement performed on X [18] (see also Appendix). This means that in

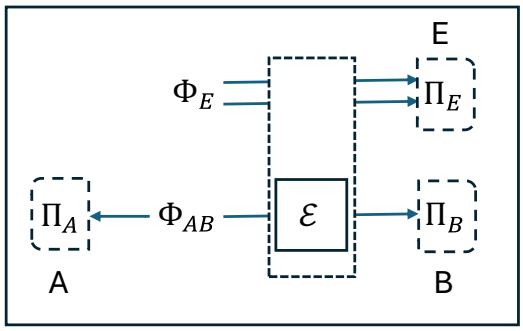


FIG. 1. Communication scheme in the entanglement-based representation. Alice sends one mode, B, of Φ_{AB} to Bob through a channel $\mathcal{E}$, while retaining mode A. Information is exchanged through measurements of the state, and guessing the outcome of either by Alice (direct reconciliation) or Bob (reverse reconciliation). The action of the channel can be interpreted as an eavesdropper, Eve, acting on an extended space to recover shared information.

this scenario the inequality is indeed saturated, i.e., we have

$$R_{XY} = \chi_Y^{\Pi_X}. \tag{2}$$

The action of a possible eavesdropper, Eve, can be analyzed by a dilation of the channel. For Gaussian channels the collective attack performed by Eve can be characterized using an input TMSV on E, Φ_E, that defines a unique dilation for the channel, $\tilde{\mathcal{E}}$, up to local unitary transformations [19]. The scheme is reported in Fig. 1. The mutual information of E and the sender system X is upper bounded by:

$$I(E:X) \leqslant \chi_E^{\Pi_X} := S(\rho_E) - \sum_x p_x S(\rho_{E|x}). \tag{3}$$

In view of the achievability of the rate in Eq. (1) (see Appendix), the rate R of private communication through the channel, that establishes a lower bound on the secret rate capacity K, is lower bounded as follows:

$$K \geqslant R \geqslant \mathcal{L} := \lim_{\mu\to\infty} \max_{\Pi_X} \chi_Y^{\Pi_X} - \chi_E^{\Pi_X}, \tag{4}$$

where for clarity we explicitly stated that the quantities are evaluated in the limit $\mu \to \infty$, and we will omit this limit hereinafter for brevity of notation.

The total local states ρ_X and ρ_E are not changed by the sender measurement, so the bound $\mathcal{L}$ can be written as:

$$\begin{aligned} \mathcal{L} &= I_{\mathcal{E}}^{\mathrm{C/RC}} + \Delta, \\ \Delta &:= \max_{\Pi_X} \sum_x p_x (S(\rho_{E|x}) - S(\rho_{Y|x})), \end{aligned} \tag{5}$$

where $I_{\mathcal{E}}^{\mathrm{C/RC}} = S(\rho_{A/B}) - S(\rho_{AB})$ is the direct or reverse coherent information of the channel [10], and we used the fact that the total state of systems ABE is pure, so that $S(\rho_E) = S(\rho_{AB})$. Note how $I_{\mathcal{E}}^{\mathrm{C/RC}}$ in itself represents a lower bound for the private capacity of the channel [10], and we will use it as a comparison for our lower bound $\mathcal{L}$, which will then be an improvement on the former if $\Delta > 0$ and $\mathcal{L} > 0$.

III. GAUSSIAN MEASUREMENTS

In the following we restrict the maximization in Eq. (4) to Gaussian measurements and we denote the restricted quantities $\mathcal{L}^G$ and Δ^G. For these measurements the conditional covariance matrix (CM) of the states, $\rho_{Y/E|x}$ will not depend on the measurement outcome x [8,20], $S(\rho_{Y/E|x}) = S(\rho_{Y/E|X})$ $\forall x$, thus:

$$\Delta^G = \max_{\Pi_X^G} S(\rho_{E|X}) - S(\rho_{Y|X}). \tag{6}$$

Let us denote the covariance matrix (CM) of the Gaussian state shared by Alice and Bob (after the channel) as:

$$\mathbf{V}_{YX} = \begin{pmatrix} \mathbf{Y} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{X} \end{pmatrix}. \tag{7}$$

A local Gaussian measurement on X can be represented as a projection on a Gaussian state ρ_0 having mean $\mathbf{x}_0 = 0$ and CM $\mathbf{V}_0$ followed by a displacement of $\mathbf{k}$, indicating the outcome of the measurement [8,20]. The state of Y conditioned to X measuring $\mathbf{k}$ is Gaussian with CM [8]:

$$\mathbf{V}_{Y|X} = \mathbf{Y} - \mathbf{C}(\mathbf{X} + \mathbf{V}_0)^{-1}\mathbf{C}^T. \tag{8}$$

Furthermore we can always decompose the single mode CM $\mathbf{V}_0$ as [8]:

$$\mathbf{V}_0(\gamma, r, \theta) = \gamma \mathbf{R}(\theta)\mathbf{S}(2r)\mathbf{R}(\theta)^T, \tag{9}$$

where $\gamma = 2n_\gamma + 1$ is the parameter of a thermal state with n_γ photons, $\mathbf{R}$ a rotation of θ and $\mathbf{S}$ a squeezing with parameter $2r$. Projecting onto coherent states, $\mathbf{V}_0 = \mathbb{1}$, corresponds to heterodyne detection, while homodyne detection is recovered in the limit of infinite squeezing. More generally, the squeezing parameter r controls how unbalanced the projection is toward one of the quadratures, while γ controls the broadening of the measurement in phase space.

The optimal attack performed by Eve depends on the channel considered, as we detail in the following. Regardless of the specific interaction, we denote the off-diagonal elements of the CM of E and X after the attack, $\mathbf{V}_{EX}$, as $\mathbf{C}_E$. In view of Eq. (8), Eve conditional CM is $\mathbf{V}_{E|X} = \mathbf{E} - \mathbf{C}_E(\mathbf{X} + \mathbf{V}_0)^{-1}\mathbf{C}_E^T$.

The entropy of a Gaussian state is completely determined by its CM, so from the analysis above, it follows that the maximization over the measurement Π_X^G of Eq. (6) can be performed over the real parameters (γ, r, θ) characterizing $\mathbf{V}_0$.

In the following we compute Δ^G, and consequently the lower bound $\mathcal{L}^G$, for the class of phase insensitive Gaussian channels, composed of thermal loss, thermal amplification and added noise. For these channels we show in Appendix that the conditioned entropies do not depend on the rotation angle θ, nor on the squeezing parameter r, so that Δ_G simplifies as:

$$\Delta^G = \max_{\gamma\geqslant 1} S(\rho_{E|X}) - S(\rho_{Y|X}), \tag{10}$$

with the maximization being only on the single real parameter $\gamma \geqslant 1$. The optimization over γ exploits the asymmetry between the conditional states of Y and E. A broader measurement can suppress Eve's information more than it degrades the rate at Y, yielding a net gain in $\mathcal{L}^G$. Note how the bound $\mathcal{L}^G$ applies either in direct or reverse reconciliation regardless of the channel, so both are computed, but we present only the one that is relevant in each case.

IV. THERMAL LOSS

A thermal loss channel, $\mathcal{E}_{\eta,\omega}$, is a Gaussian channel characterized by parameters $0 < \eta < 1$, representing the transmissivity and $\omega = 2n_{\rm th} + 1 > 1$, where $n_{\rm th} > 0$ is the average number of thermal photons. This channel acts on a single-mode Gaussian state of mean $\mathbf{x}$ and CM $\mathbf{V}$ with the following input-output relations:

$$\mathbf{x} \to \sqrt{\eta}\mathbf{x}, \quad \mathbf{V} \to \eta\mathbf{V} + (1-\eta)\omega\mathbb{1}. \tag{11}$$

The maximum rate in this case is obtained by a reverse reconciliation protocol. The reverse coherent information is [11]:

$$I^{\rm RC}_{\eta,\omega} = -\log_2(1-\eta) - h(\omega). \tag{12}$$

Eve's optimal attack is a collective attack, that for the thermal loss channel consists of an entanglement cloner, detailed in the Appendix. The conditional entropies $S(\rho_{A/E|x})$ can be computed from the CMs $\mathbf{V}_{Y/E|X}$, to yield:

$$\Delta^G_{\eta,\omega} = \max_{\gamma>1} h(\lambda^{(E)}_+) + h(\lambda^{(E)}_-) - h\left(\frac{\gamma + (1-\eta)\omega}{\eta}\right), \tag{13}$$

where $h(x) = \frac{x+1}{2}\log_2[(x+1)/2] - \frac{x-1}{2}\log_2[(x-1)/2]$ is the thermal entropy function and $\lambda^{(E)}_\pm$ are the symplectic eigenvalues of $\mathbf{V}_{E|X}$ (see Appendix for detailed expressions). The maximization over γ is evaluated numerically. Let us denote the maximum amount of noise $\omega_{\rm th}(\eta)$ such that $\mathcal{L}^G_{\eta,\omega} > 0$, as the security threshold. In Fig. 2(a) we plot $\omega_{\rm th}(\eta)$ as a function of the transmissivity η and compare it to the security threshold of $I^{\rm RC}_{\mathcal{E}_{\eta,\omega}}$, showing that $\mathcal{L}^G_{\eta,\omega}$ is indeed a tighter bound than the former. In Fig. 2(b) we plot the bound as a function of η at a fixed value of ω. We compare $\mathcal{L}^G_{\eta,\omega}$ with $I^{\rm RC}_{\mathcal{E}_{\eta,\omega}}$, as well as with the bound of Ref. [21], that we denote as $\mathcal{B}_{\eta,\omega}$, and the one from Ref. [22], denoted $\mathcal{Q}_{\eta,\omega}$ that, to the best of our knowledge, jointly make up the best lower bound up to date on the secret key capacity of the thermal loss channel. We also plot the upper bound on the capacity, $\mathcal{U}_{\eta,\omega} = -\log_2[(1-\eta)^{n_{\rm th}}] - h(\omega)$ [10], as a reference. Our lower bound, $\mathcal{L}^G_{\eta,\omega}$, improves on the reverse coherent information, as expected. Notably, the protocol achieving $\mathcal{B}_{\eta,\omega}$ is a special case of our general protocol. Our results show that the former achieves the optimal performance for a fully Gaussian protocol with single-mode measurements. On the other hand, $\mathcal{Q}_{\eta,\omega}$ still provides a slightly better bound for lower values of η.

V. THERMAL AMPLIFICATION

A thermal amplification channel, $\mathcal{E}_{g,\omega}$, is defined by the parameters $g > 1$, and $\omega = 2n_{\rm th} + 1 > 1$. The input-output relations of this channel are

$$\mathbf{x} \to \sqrt{g}\mathbf{x} \quad \mathbf{V} \to g\mathbf{V} + (g-1)\omega\mathbb{1}, \tag{14}$$

Eve's optimal attack is the same of the previous section, an entanglement cloner. In the case of amplification however, the best performance is obtained in direct reconciliation, and the coherent information of the channel is

$$I^C_{g,\omega} = -\log_2\left(\frac{g}{g-1}\right) - h(\omega), \tag{15}$$

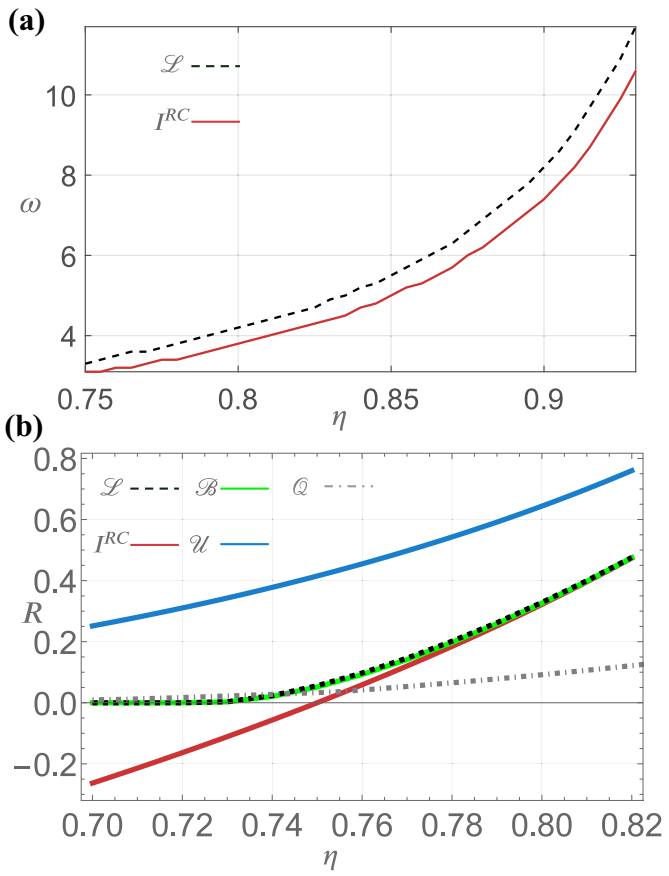


FIG. 2. Thermal loss channel. (a) We plot the security threshold $\omega_{\rm th}$, defined in the main text, as a function of the transmissivity η, for the bound $\mathcal{L}_{\eta,\omega}$ and the channel's reverse coherent information $I^{\rm RC}_{\eta,\omega}$. (b) $\mathcal{L}_{\eta,\omega}$ is compared with the lower bounds $\mathcal{B}_{\eta,\omega}$ and $\mathcal{Q}_{\eta,\omega}$ (see the main text) at a fixed value $\omega = 3$. We also plot $I^{\rm RC}_{\eta,\omega}$ as well as the upper bound on the capacity $\mathcal{U}_{\eta,\omega}$.

the calculation of the Δ term yields:

$$\Delta^G_{g,\omega} = \max_{\gamma>1} h(\lambda^{(E)}_+) + h(\lambda^{(E)}_-) - h(\gamma g - \omega + g\omega), \tag{16}$$

where once again we report the symplectic eigenvalues in Appendix.

In Fig. 3 we report the same plots of the previous section. Namely, in Fig. 3(a) we plot the security threshold $\omega_{\rm th}(g)$ of $\mathcal{L}^G_{g,\omega}$ and $I^C_{g,\omega}$. In Fig. 3(b) we compare $\mathcal{L}^G_{g,\omega}$ at a fixed value of ω to the best known bounds, taken from Ref. [23], denoted $\mathcal{B}_{g,\omega}$, and Ref. [22], denoted $\mathcal{Q}_{g,\omega}$, and with the upper bound on the capacity $\mathcal{U} = I^C_{g,\omega} = -\log_2(\frac{g^{n_{\rm th}}}{g-1}) - h(\omega)$. The results for thermal amplification are similar to the ones for thermal loss, with $\mathcal{L}^G_{g,\omega}$ saturated by $\mathcal{B}_{g,\omega}$, thus showing the optimality of the protocol in Ref. [23], within the restriction of our analysis, and $\mathcal{Q}_{g,\omega}$ being a small improvement for higher values of g.

VI. ADDED NOISE

An added noise channel, $\mathcal{E}_\zeta$, adds $\zeta > 0$ thermal photons, representing classical noise, to the input signal. The input is transformed according to $\mathbf{x} \to \mathbf{x}$ and $\mathbf{V} \to \mathbf{V} + 2\zeta\mathbb{1}$. The best lower bound for the private capacity of the channel is given by

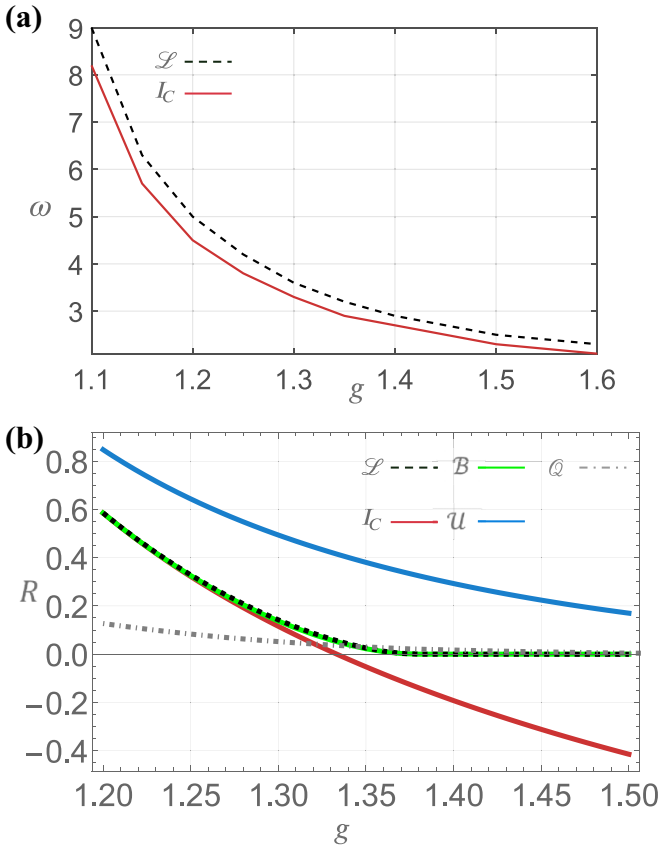


FIG. 3. Thermal amplification. (a) Security threshold ω_{th}, for the thermal amplification channel (see main text) as a function of the gain g, for the bound $\mathcal{L}_{\omega,g}$ and the coherent information of the channel $I^C_{\omega,g}$. (b) Comparison of $\mathcal{L}_{\omega,g}$ with the lower bounds $\mathcal{B}_{\omega,g}$ and $\mathcal{Q}_{\omega,g}$ (see the main text) at $\omega = 3$ with $I^{\text{RC}}_{\eta,\omega}$ and the upper bound $\mathcal{U}_{\omega,\eta}$ as reference.

the coherent information [11]:

$$I^C_\zeta = -\frac{1}{\log(2)} - \log_2(\zeta). \tag{17}$$

We point out that for this channel the same lower bound is obtained by the reverse coherent information, $I^{\text{RC}}_\zeta = I^C_\zeta$ since they are computed in the limit $\mu \to \infty$. The quantity Δ^G_ζ can then be computed either in direct or reverse reconciliation, but both configurations yield the same result. For this channel the best collective attack is a universal cloner [19,24], different from the entanglement cloner of the previous section, as detailed in Appendix. For the channel $\mathcal{E}_\zeta$ we compute:

$$\Delta^G_\zeta = \max_{\gamma>1} h(\lambda^{(E)}_+) + h(\lambda^{(E)}_-) - h(2\zeta+\gamma), \tag{18}$$

where $\lambda^{(E)}_\pm$ are reported in Appendix.

In Fig. 4(a) we plot $\mathcal{L}^G_\zeta$ as a function of ζ and compare it to I^C_ζ and the lower bound of Ref. [22], denoted as $\mathcal{Q}_\zeta$. The plot shows how the former is an improvement on the latter for lower values of ζ. We also report the upper bound on the capacity, $\mathcal{U} = (\zeta-1)/\log(2) - \log_2(\zeta)$ [10], as a reference.

The improvement over the coherent information is further shown in Fig. 4(b) where we plot the argument of Eq. (18),

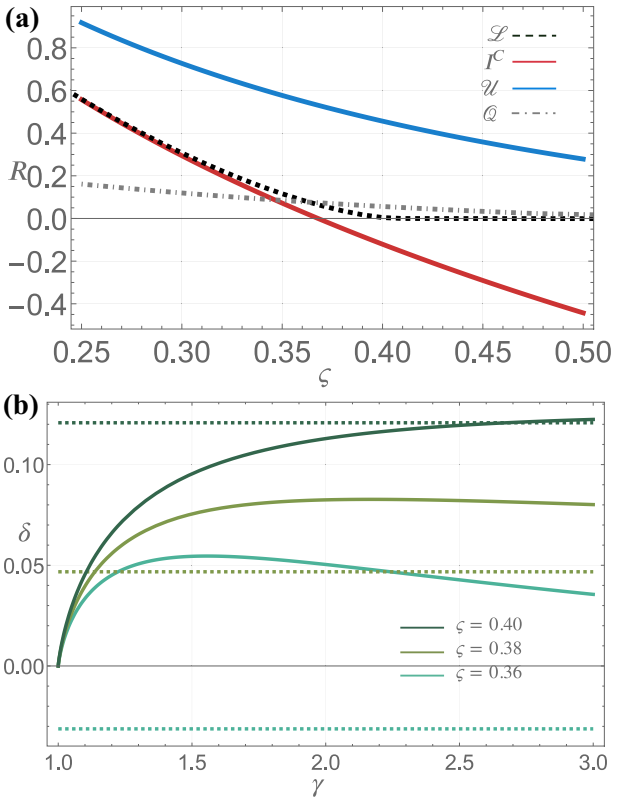


FIG. 4. Added noise. (a) Comparison of the bound $\mathcal{L}^G_\zeta$ with I^C_ζ and $\mathcal{Q}_\zeta$. The upper bound $\mathcal{U}_\zeta$ is also reported for reference. (b) $\delta(\gamma)$ (see main text) is plotted for parameters $\bar{\zeta} = 0.36, 0.38, 0.40$. The value of $-I^C_\zeta$ is reported for reference in dashed lines.

$\delta(\gamma) := h(\lambda^{(E)}_+) + h(\lambda^{(E)}_-) - h(2\zeta+\gamma)$, for fixed values $\bar{\zeta} = 0.36, 0.38, 0.40$, as a function of the optimization parameter $\gamma \geqslant 1$. Since the improvement is significant only when $I^C_\zeta + \delta(\gamma,\zeta) > 0$ we also report the value $-I^C_{\bar{\zeta}}$, in dashed lines for each value of $\bar{\zeta}$, providing a visualization of the range of parameters γ for which the bound is effectively tighter. Our bound thus provides an improvement, albeit small, over all previously known lower bounds.

VII. CONCLUSIONS

We analyzed a general protocol in which private communication between two parties is performed by locally measuring a bipartite state shared via a quantum channel $\mathcal{E}$, aided by one way classical communication. We provided a lower bound on the achievable secret key rate of this scheme, that in turn gives a lower bound on the secret key capacity of the channel. We focused our analysis on phase insensitive Gaussian channels and restricted the measurements to single-mode Gaussian ones. Our analysis finds a relatively simple formula for a lower bound of the secret key capacity involving an optimization over a single real parameter. This lower bound shows the optimality, under the aforementioned conditions, of previously proposed protocols for the thermal loss and thermal amplification channels and further gives an improved lower bound for the additive noise channel.

The analysis presented here can be expanded to other channels besides phase-insensitive ones, and further enhanced by

dropping the restriction of Gaussian measurements. Another promising development would be to consider a similar scheme that allows multimode measurements.

ACKNOWLEDGMENTS

UKRI supported this work through the Integrated Quantum Networks (IQN) Research Hub (EPSRC, Grant No. EP/Z533208/1). G.O. and L.B. acknowledge financial support from: PNRR Ministero Università e Ricerca Project No. PE0000023-NQSTI, funded by European Union-Next-Generation EU, the European Union's Horizon Europe research and innovation program under EPIQUE Project GA No. 101135288. The authors thank Francesco Anna Mele for sharing code with us to reproduce the results of Ref. [22]. The authors also thank Matthew Barber for pointing out typos in the eigenvalue formulas reported in Appendix of the first preprint version of this work. The results were unaffected.

DATA AVAILABILITY

There are no publicly available research data or software supporting this paper. Requests for further information or data should be sent to the authors.

APPENDIX: OPTIMIZATION OVER GAUSSIAN MEASUREMENTS

In the protocol of the main text we denote the party performing the measurement X and the receiving end of the communication Y, while the eavesdropper is denoted as E. According to Eq. (6) the quantity Δ_G is fully determined by the conditioned entropy terms $S(\rho_{Y/E|X})$. Since our protocol is fully Gaussian, the states $\rho_{Y/E|X}$ will be Gaussian as well and $S(\rho_{Y/E|X})$ is, in turn, fully determined by the CM $\mathbf{V}_{Y/E|X}$. Let us denote the terms of the bipartite CM $\mathbf{V}_{(Y/E)X}$ after the channel $\mathcal{E}$ as:

$$\mathbf{V}_{(Y/E)X} = \begin{pmatrix} \mathbf{Y/E} & \mathbf{C}_{Y/E} \\ \mathbf{C}_{Y/E}^T & \mathbf{X} \end{pmatrix}. \tag{A1}$$

After a Gaussian measurement on X the conditioned local CM is

$$\mathbf{V}_{D|X} = \mathbf{D} - \mathbf{C}(\mathbf{X} + \mathbf{V}_0)^{-1}\mathbf{C}^T, \tag{A2}$$

where $D = Y/E$, $\mathbf{C} = \mathbf{C}_{Y/E}$ and $\mathbf{V}_0$ is the CM of a zero mean Gaussian state determining the measurement performed. As stated in the main text we can decompose $\mathbf{V}_0$ as:

$$\mathbf{V}_0(\gamma, r, \theta) = \gamma \mathbf{R}(\theta)\mathbf{S}(2r)\mathbf{R}(\theta)^T. \tag{A3}$$

Using this decomposition the measurement Π_X^G is determined by the parameters (γ, r, θ). Let us denote the argument of the maximization of Δ_G as $\delta(\gamma, r, \theta) := S(\rho_{E|X}) - S(\rho_{Y|X})$.

To derive Eq. (10) we start by showing that δ does not depend on θ. Consider the following equality:

$$\begin{aligned} &\mathbf{C}(\mathbf{D} + \gamma \mathbf{R}(\theta)\mathbf{S}(2r)\mathbf{R}(\theta)^T)^{-1}\mathbf{C}^T \\ &\quad = \mathbf{C}\mathbf{R}(\theta)(\mathbf{R}(\theta)^T\mathbf{X}\mathbf{R}(\theta) + \gamma \mathbf{S}(2r))^{-1}\mathbf{R}(\theta)^T\mathbf{C}^T, \end{aligned} \tag{A4}$$

where we used the orthogonality of $\mathbf{R}(\theta)$, $\mathbf{R}(\theta)\mathbf{R}(\theta)^T = \mathbb{1}$. In the protocol analyzed, the initial states are fixed to Φ_A and Φ_E so after a phase-insensitive channel $\mathbf{R}(\theta)^T\mathbf{D}\mathbf{R}(\theta) = \mathbf{D}$. For the same reason $\mathbf{C}_Y \propto \mathbf{Z} = \mathrm{diag}(1, -1)$, so that $\mathbf{R}(\theta)\mathbf{C}_Y\mathbf{R}(\theta) = \mathbf{C}_Y$. We have then:

$$\mathbf{R}(\theta)\mathbf{V}_{Y|X}\mathbf{R}(\theta)^T = \mathbf{Y} - \mathbf{C}_Y(\mathbf{X} + \gamma \mathbf{S}(2r))^{-1}\mathbf{C}_Y^T. \tag{A5}$$

In other words the parameter θ determines a unitary local rotation on the conditioned CMs $\mathbf{V}_{Y|X}$ and does not alter its entropy. For system E we note that $\mathbf{C}_E = \binom{\mathbf{C}_1}{\mathbf{C}_2}$ where the composing blocks are proportional to either $\mathbf{Z}$ or $\mathbb{1}$. This means that there exists a local unitary, $\mathbf{R}_2(\theta_1, \theta_2) := \mathbf{R}(\theta_1) \oplus \mathbf{R}(\theta_2)$, on E such that:

$$\mathbf{R}_2(\theta_1, \theta_2)\mathbf{V}_{E|X}\mathbf{R}_2(\theta_1, \theta_2)^T = \mathbf{E} - \mathbf{C}_E(\mathbf{X} + \gamma \mathbf{S}(2r))^{-1}\mathbf{C}_E^T, \tag{A6}$$

where θ_1, θ_2 are either θ or $-\theta$. This means that the conditional entropy on E does not depend on θ as well. Consequently, for phase-insensitive channels, $\delta(\gamma, r, \theta)$ does not depend on θ, $\delta(\gamma, r, \theta) = \delta(\gamma, r)$.

On the other hand, the dependence of $\delta(\gamma, r)$ on the squeezing parameter r is not trivial. While one might expect $r = 0$ to be optimal for phase-insensitive channels on symmetry grounds, this is not guaranteed *a priori*, as the optimization also involves Eve's side and the interplay between the entropy terms. We analytically verify that $\partial_r \delta(\gamma, r)|_{r=0} = 0$ and $\partial_r^2 \delta(\gamma, r)|_{r=0} < 0$, establishing that $r = 0$ is a local maximum. We verify by numerical analysis that the maximum is indeed global. Thus we have:

$$\Delta^G = \max_{\gamma \geqslant 1} \delta(\gamma, 0), \tag{A7}$$

that is Eq. (10) of the main text.

1. Collective attacks

For the sake of security analysis, a quantum channel can be interpreted as the effect of an Eavesdropper's, Eve, attack on the transmission. This is done by considering a dilation of the channel to a larger space with the assumption that this larger space is under Eve's control. We consider collective attacks meaning that Eve' state is stored in a quantum memory for the duration of the communication and global measurements are performed at the end of the protocol. In this scenario Eve' recovered information is upper bounded by the conditioned χ quantity, $\chi_{E|X}$, to the classical information X as discussed in the main text. Collective attacks on Gaussian channel are fully characterized in terms of the Stinespring dilation where Eve's input state is a TMSV state of parameter ω [19].

For the thermal loss and thermal amplification channels, $\mathcal{E}_{\omega,\eta/g}$, this dilation is similarly constituted of an entanglement cloner [19]. This consist in a two mode interaction, a beam splitter or thermal amplifier with transmissivity or amplification, $0 \leqslant \eta \leqslant 1$ or $g > 1$, respectively. As reported in Fig. 5(a) one mode of Eve's TMSV state enters the second port of the beam splitter or amplifier while the other mode is kept for joint measurements.

For the added noise channel, $\mathcal{E}_\zeta$, the optimal collective attack is a universal cloner [24]. It consists in an irreducible three mode channel composed by a sequence of cv-CNOT gates [25]. A continuous variable CNOT in the phase space is a unitary operation acting on the quadratures of two modes,

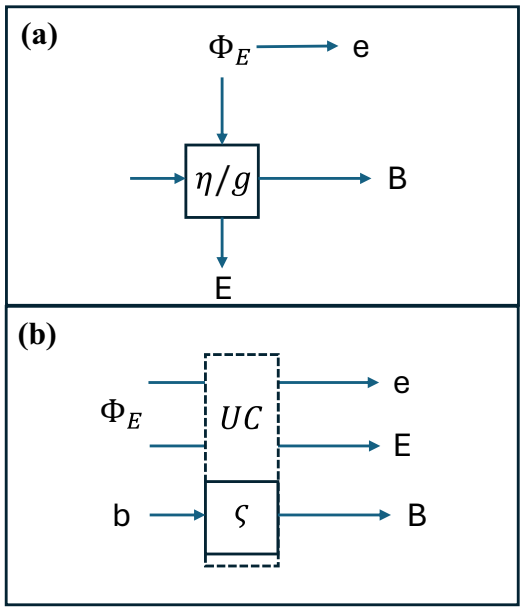


FIG. 5. Dilation of the channels. (a) Thermal loss and thermal amplification are dilated by a beam splitter or thermal amplifier with parameter η/g. The dilation consists of a two-mode interaction between B and E, while e is stored for later measurement. (b) The dilation of an added noise channel is a universal cloner, a three-mode interaction involving e, E, and B, described by the unitary in Eq. (A9).

$\{\hat{x}_j, \hat{p}_j\}$, as:

$$U_{\text{CNOT}} = e^{-ic\hat{x}_1\hat{p}_2}, \tag{A8}$$

with the real parameter c determining the strength of the interaction. Referring to the scheme in Fig. 5(b) for the labeling of the modes, the universal cloner acts as [24]:

$$U_{\text{UC}} = e^{-i(\hat{x}_e-\hat{x}_E)\hat{p}_B} e^{-i\hat{x}_B(\hat{p}_e-\hat{p}_E)}. \tag{A9}$$

The CM of the full system evolves according to $\mathbf{V}_{eEB} \to \mathbf{L}_{\text{UC}}\mathbf{V}_{eEB}\mathbf{L}_{\text{UC}}^T$, where $\mathbf{L}_{\text{UC}}$ is the symplectic matrix associated with U_{UC}:

$$\mathbf{L}_{\text{UC}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 5 & 0 & 4 & 0 & -2 \\ 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & -4 & 0 & -3 & 0 & 2 \\ 2 & 0 & -2 & 0 & 1 & 0 \\ 0 & -2 & 0 & -2 & 0 & 1 \end{pmatrix}. \tag{A10}$$

The local action on B of this transformation is:

$$\mathbf{B} \to \mathbf{B} + 2(4\omega - 4\sqrt{\omega^2-1})\mathbb{1}, \tag{A11}$$

that is an added noise channel with parameter $\zeta = 4\omega - 4\sqrt{\omega^2-1}$.

2. Symplectic eigenvalues

In this section we present the expressions for the symplectic eigenvalues of Eve conditional CV, used in the main text, for each of the channels.

(a) Thermal loss:

$$\lambda_{\pm}^{(E)} = \frac{\sqrt{[(1-\eta)\gamma + (1+\eta)\omega]^2 - 4\eta(\omega^2-1)} \pm (1-\eta)(\gamma+\omega)}{2\eta}.$$

(b) Thermal amplification:

$$\lambda_{\pm}^{(E)} = \frac{\sqrt{[(g-1)\gamma + (g+1)\omega]^2 - 4g(\omega^2-1)} \pm (g-1)(\gamma+\omega)}{2}.$$

(c) Added noise:

$$\lambda_{\pm}^{(E)} = \sqrt{\zeta^2 + 2\gamma\zeta + 1} \pm \zeta.$$

3. Secret key rate

We lower bound the optimal secret key rate in the asymptotic regime of a large number of uses of the channel. Following the notation of the main text we label the party performing the measurement as X, and the other party as Y. Let us fix the measurement Π_X, yielding the classical random variable $\mathbf{x}$ on system X. Communication is achieved by subsequent measurements on Y, aided by one way classical communication. For the classical-quantum system XY the maximum common randomness that can be extracted with unlimited one-way classical communication is given by the classical-quantum Slepian-Wolf result [26] (see also Lemma 4 of Ref. [18]), stating that $S(\mathbf{x}|Y)$ bits of public communication are needed from X to Y, for the latter to reproduce $\mathbf{x}$ (in the asymptotic limit of many copies). This yields a raw key rate:

$$R_{XY} = H(\mathbf{x}) - S(\mathbf{x}|Y) = I(\mathbf{x}:Y), \tag{A12}$$

where $S(\mathbf{x}|Y)$ are the bits of public communication and thus subtracted from the key, and $I(\mathbf{x}:Y)$ is the mutual information of the classical quantum system XA, equal to the Holevo quantity $\chi_Y^{\Pi_X}$, i.e., $I(\mathbf{x}:Y) = \chi_Y^{\Pi_X}$. After a collective attack by Eve the optimal asymptotic secret key rate, R^{Π_X}, is lower bounded using the above raw key rate and the classical Csiszar-Korner theorem by the quantity [6,27]:

$$R^{\Pi_X} \geqslant R_{XY} - I(\mathbf{x}:E), \tag{A13}$$

where $I(\mathbf{x}:E) = \chi_E^{\Pi_X}$ serves as an upper limit on the information extracted by Eve regardless of measurement and postprocessing. Maximizing the rate in Eq. (A13) over Π_x, in the limit of $\mu \to \infty$, gives our lower bound in Eq. (4).

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proceedings of the IEEE International Conference on Computers* (Systems and Signal Processing, Bangalore, 1984), pp. 175–179.
[2] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).
[3] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, Phys. Rev. Lett. **88**, 057902 (2002).
[4] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, Nature (London) **421**, 238 (2003).
[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).
[6] 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. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).
[7] S. L. Braunstein and P. van Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513 (2005).
[8] 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).
[9] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods*, 1st ed. (CRC Press, Boca Raton, 2017).
[10] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nature Commun. **8**, 15043 (2017).
[11] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Direct and reverse secret-key capacities of a quantum channel, Phys. Rev. Lett. **102**, 050503 (2009).
[12] B. Schumacher and M. A. Nielsen, Quantum data processing and error correction, Phys. Rev. A **54**, 2629 (1996).
[13] S. Lloyd, Capacity of the noisy quantum channel, Phys. Rev. A **55**, 1613 (1997).
[14] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, Reverse coherent information, Phys. Rev. Lett. **102**, 210501 (2009).
[15] V. Vedral, M. B. Plenio, K. Jacobs, and P. L. Knight, Statistical inference, distinguishability of quantum states, and quantum entanglement, Phys. Rev. A **56**, 4452 (1997).
[16] V. Vedral and M. B. Plenio, Entanglement measures and purification procedures, Phys. Rev. A **57**, 1619 (1998).
[17] M. B. Plenio and V. Vedral, Bounds on relative entropy of entanglement for multi-party systems, J. Phys. A: Math. Gen. **34**, 6997 (2001).
[18] I. Devetak and A. Winter, Distilling common randomness from bipartite quantum states, IEEE Trans. Inf. Theory **50**, 3183 (2004).
[19] 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).
[20] S. Pirandola, G. Spedalieri, S. L. Braunstein, N. J. Cerf, and S. Lloyd, Optimality of Gaussian discord, Phys. Rev. Lett. **113**, 140405 (2014).
[21] C. Ottaviani, R. Laurenza, T. P. W. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Secret key capacity of the thermal-loss channel: Improving the lower bound, in *SPIE Proceedings* (SPIE, Bellingham, 2016), Vol. 9996, p. 999609.
[22] F. A. Mele, L. Lami, and V. Giovannetti, Maximum tolerable excess noise in continuous-variable quantum key distribution and improved lower bound on two-way capacities, Nat. Photon. **19**, 329 (2025).
[23] G. Wang, C. Ottaviani, H. Guo, and S. Pirandola, Improving the lower bound to the secret-key capacity of the thermal amplifier channel, Eur. Phys. J. D **73**, 17 (2019).
[24] N. J. Cerf, A. Ipe, and X. Rottenberg, Cloning of continuous quantum variables, Phys. Rev. Lett. **85**, 1754 (2000).
[25] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Efficient classical simulation of continuous variable quantum information processes, Phys. Rev. Lett. **88**, 097904 (2002).
[26] I. Devetak and A. Winter, Classical data compression with quantum side information, Phys. Rev. A **68**, 042301 (2003).
[27] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. (Cambridge University Press, Cambridge, 2011).