12-19-2017

Upper bounds on secret-key agreement over lossy thermal bosonic channels

Eneet Kaur
Hearne Institute for Theoretical Physics

Mark M. Wilde
Hearne Institute for Theoretical Physics

Recommended Citation

Kaur, E., & Wilde, M. (2017). Upper bounds on secret-key agreement over lossy thermal bosonic channels. *Physical Review A, 96* (6) https://doi.org/10.1103/PhysRevA.96.062318

Upper bounds on secret-key agreement over lossy thermal bosonic channels

Eneet Kaur and Mark M. Wilde

Phys. Rev. A **96**, 062318 — Published 19 December 2017

DOI: 10.1103/PhysRevA.96.062318

Upper bounds on secret key agreement over lossy thermal bosonic channels

Eneet Kaur
Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Baton Rouge, Louisiana 70803, USA

Mark M. Wilde
Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Baton Rouge, Louisiana 70803, USA and Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA

(Dated: November 29, 2017)

Upper bounds on the secret-key-agreement capacity of a quantum channel serve as a way to assess the performance of practical quantum-key-distribution protocols conducted over that channel. In particular, if a protocol employs a quantum repeater, achieving secret-key rates exceeding these upper bounds is a witness to having a working quantum repeater. In this paper, we extend a recent advance [Liuzzo-Scorpo *et al.*, Phys. Rev. Lett. 119, 120503 (2017)] in the theory of the teleportation simulation of single-mode phase-insensitive Gaussian channels such that it now applies to the relative entropy of entanglement measure. As a consequence of this extension, we find tighter upper bounds on the non-asymptotic secret-key-agreement capacity of the lossy thermal bosonic channel than were previously known. The lossy thermal bosonic channel serves as a more realistic model of communication than the pure-loss bosonic channel, because it can model the effects of eavesdropper tampering and imperfect detectors. An implication of our result is that the previously known upper bounds on the secret-key-agreement capacity of the thermal channel are too pessimistic for the practical finite-size regime in which the channel is used a finite number of times, and so it should now be somewhat easier to witness a working quantum repeater when using secret-key-agreement capacity upper bounds as a benchmark.

I. INTRODUCTION

One of the main goals of quantum information theory [1–3] is to establish bounds on communication rates for various information-processing tasks. An important application lies in the domain of secret communication, following the development of quantum key distribution [4, 5]. In recent years, there has been a growing interest in establishing bounds on the secret-key-agreement capacity of a quantum channel, which is the highest rate at which communicating parties can use the channel and public classical communication to distill a secret key [6–18]. Such bounds have been proven by exploiting the methods of quantum information theory and can be interpreted as setting the fundamental limitations of quantum key distribution whenever a quantum repeater is not available [19].

An important development occurred in [7], in which it was established that there is a fundamental rate-loss trade-off that any repeaterless quantum key distribution protocol cannot overcome. That is, without a quantum repeater, the rate of secret key that can be distilled from a pure-loss bosonic channel (lossy optical fiber or a free-space channel) decreases exponentially with increasing distance [7].

Later, this bound was improved to establish that the secret-key-agreement capacity of a pure-loss bosonic channel of transmissivity $\eta \in (0,1)$ is equal to $-\log_2(1-\eta)$. This bound was claimed in [9] and rigorously proven in [13]. In particular, let $P^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon)$ denote the highest rate at which ε-close-to-ideal secret key can be distilled by making n invocations of a pure-loss channel $\mathcal{L}_\eta$ of transmissivity η, along with the assistance of public classical communication [13]. In [13], $P^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon)$ is called the non-asymptotic secret-key-agreement capacity of the channel $\mathcal{L}_\eta$. One of the results of [13] is the following fundamental upper bound:

$$P^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq -\log_2(1-\eta) + \frac{C(\varepsilon)}{n}, \tag{1}$$

where $C(\varepsilon) = \log_2 6 + 2\log_2([1+\varepsilon]/[1-\varepsilon])$. The bound in (1) is known as a strong converse bound because it converges to the secret-key-agreement capacity $-\log_2(1-\eta)$ in the limit as $n \to \infty$. We suspect that there is little room for improvement of the bound in (1) and discuss this point further in Appendix A. The bound in (1) is to be contrasted with the following weak-converse bound:

$$P^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \frac{1}{1-\varepsilon}\left[-\log_2(1-\eta) + \frac{h_2(\varepsilon)}{n}\right], \tag{2}$$

which follows as a direct consequence of [13, Section 8] and [20, Eq. (2)] (see also [21, Eq. (134)]). For the benefit of the reader, we explain how to arrive at this weak-converse bound in more detail in Appendix B. In the above,

$$h_2(\varepsilon) = -\varepsilon\log_2\varepsilon - (1-\varepsilon)\log_2(1-\varepsilon) \tag{3}$$

denotes the binary entropy. The bound in (2) is a weak-converse bound because it requires the extra limit as $\varepsilon \to 0$ after taking the limit as $n \to \infty$, in order to arrive at the capacity upper bound of $-\log_2(1-\eta)$. The significance of the bounds in (1) and (2) is that they apply for any finite number n of channel uses and key-quality parameter ε. As such, these bounds can be used to assess the performance of any practical secret-key-agreement protocol conducted over a pure-loss channel $\mathcal{L}_\eta$.

The pure-loss channel is somewhat of an ideal model for a communication channel, even if it does have a strong physical underpinning in the context of free-space communication [22, 23]. In particular, a working assumption of the model is that the channel input interacts with an environment prepared in the vacuum state. However, in practical setups, we might expect the environment to be modeled as a thermal state of a fixed mean photon number $N_B > 0$ [23], and in such a case, the channel is called a thermal channel and denoted by $\mathcal{L}_{\eta,N_B}$ (also called thermal-lossy channel, as in [17]). This added thermal noise is often called excess noise [24, 25], which can serve as a simple model of tampering by an eavesdropper. Additionally, there are realistic effects in communication schemes, such as dark counts of photon detectors that can be modeled as arising from thermal photons in the environment [17, 23]. As such, it is an important goal to establish upper bounds on the secret-key-agreement capacity of the thermal channel in order to assess the performance of practical secret-key-agreement protocols, and the main contribution of the present paper is to establish upper bounds on the non-asymptotic secret-key-agreement capacity $P^{\leftrightarrow}_{\mathcal{L}_{\eta,N_B}}(n,\varepsilon)$ of the thermal channel $\mathcal{L}_{\eta,N_B}$, which improve upon the prior known bounds from [9, 13] in certain regimes.

Prior works established that

$$-\log_2([1-\eta]\,\eta^{N_B}) - g(N_B) \tag{4}$$

is an upper bound on the secret-key-agreement capacity of a thermal channel $\mathcal{L}_{\eta,N_B}$ with transmissivity $\eta \in (0,1)$ and thermal mean photon number $N_B > 0$. This bound was claimed in [9] and rigorously proven in [13]. In this expression,

$$g(N_B) = (N_B+1)\log_2(N_B+1) - N_B \log_2 N_B \tag{5}$$

is the entropy of a thermal state of mean photon number N_B. In particular, the following bound was given in [13, Section 8]

$$P^{\leftrightarrow}_{\mathcal{L}_{\eta,N_B}}(n,\varepsilon) \leq -\log_2([1-\eta]\,\eta^{N_B}) - g(N_B) + \sqrt{\frac{2V_{\eta,N_B}}{n\,(1-\varepsilon)}} + \frac{C(\varepsilon)}{n}, \tag{6}$$

where

$$V_{\eta,N_B} = N_B(N_B+1)\log_2^2(\eta\,[N_B+1]\,/N_B), \tag{7}$$

and the following weak-converse bound is a direct consequence of [13, Section 8] and [20, 21] (explained also in Appendix B):

$$P^{\leftrightarrow}_{\mathcal{L}_{\eta,N_B}}(n,\varepsilon) \leq \frac{1}{1-\varepsilon}\left[-\log_2([1-\eta]\,\eta^{N_B}) - g(N_B) + \frac{h_2(\varepsilon)}{n}\right]. \tag{8}$$

Again, the value of these bounds is that they apply for any finite number n of channel uses and key-quality parameter ε. However, by inspecting (6), we see that the order $1/\sqrt{n}$ and lower terms are strictly positive.

The main contribution of the present paper is to improve the bound in (6) in such a way that the order $1/\sqrt{n}$ term is negative whenever $\varepsilon < 1/2$, representing the back-off from capacity incurred by using the channel a finite number of times while allowing for non-zero error. In fact, we find the following improved bound for several realistic values of η and N_B:

$$P^{\leftrightarrow}_{\mathcal{L}_{\eta,N_B}}(n,\varepsilon) \leq -\log_2([1-\eta]\,\eta^{N_B}) - g(N_B) + \sqrt{\frac{V'_{\eta,N_B}}{n}}\Phi^{-1}(\varepsilon) + \frac{O(\log n)}{n}, \tag{9}$$

where V'_{η,N_B} is a channel-dependent parameter that we discuss later and Φ^{-1} denotes the inverse of the cumulative normal distribution function (see (41)), for which we have that $\Phi^{-1}(\varepsilon) < 0$ whenever $\varepsilon < 1/2$. We should note that the bound in (9) applies only for n sufficiently large (such that n is proportional to $1/\varepsilon^2$), as it relies on the Berry–Esseen theorem [27, 28], but many prior works have shown that first- and second-order terms like the above one serve as an excellent approximation for non-asymptotic capacities even for small n [21, 29–32]. The main new tool that we use to establish this result, beyond those used and introduced in [13], is a recent development in [26] regarding teleportation simulation of single-mode phase-insensitive bosonic channels using finite-energy resource states. Figure 1 plots this bound for several realistic values of the distance L (related to transmissivity η) and thermal mean photon number N_B, and we point to Section IV for a more detailed discussion of these figures.

In the prior work [13], it was not possible to establish a result of the form in (9) because the limiting resource state used for teleportation was an ideal, infinite-energy state. Thus, it was not clear how to invoke the Berry-Esseen theorem then because it was not clear how to prove that the quantity $T(\rho\|\sigma)$ (discussed later in (39)) is finite in such a case. However, now that the resource state can be a finite-energy state (due to the results of [26]), it is possible to establish that the quantity $T(\rho\|\sigma)$ is finite in such a case, and this is what is accomplished and discussed in Appendix D.

In the remainder of the paper, we argue how to arrive at the bound in (9). We first review the formalism of quantum Gaussian states and channels [33, 34], and we also review information quantities needed, such as quantum relative entropy and relative entropy variance. We then review the critical tool of teleportation simulation of a quantum channel [35–39] and how it can be used with [13, Eq. (4.34)] and ideas from [26] in order to arrive at (9). We finally close with a summary and some open questions.

II. PRELIMINARIES

A. Quantum Gaussian states and channels

The main class of quantum states in which we are interested in this paper are quantum Gaussian states [33, 34]. In our brief review, we consider m-mode Gaussian states, where m is some fixed positive integer. Let $\hat{x}_j$ denote each quadrature operator ($2m$ of them for an m-mode state), and let $\hat{x} \equiv [\hat{q}_1, \ldots, \hat{q}_m, \hat{p}_1, \ldots, \hat{p}_m] \equiv [\hat{x}_1, \ldots, \hat{x}_{2m}]$ denote the vector of quadrature operators, so that the first m entries correspond to position-quadrature operators and the last m to momentum-quadrature operators. The quadrature operators satisfy the following commutation relations:

$$[\hat{x}_j, \hat{x}_k] = i\Omega_{j,k}, \quad \text{where} \quad \Omega = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \otimes I_m, \tag{10}$$

and I_m is the $m \times m$ identity matrix. We also take the annihilation operator $\hat{a} = (\hat{q} + i\hat{p})/\sqrt{2}$. Let ρ be a Gaussian state, with the mean-vector entries $\langle \hat{x}_j \rangle^\rho = \mu_j^\rho$, and let μ^ρ denote the mean vector. The entries of the covariance matrix V^ρ of ρ are given by

$$V_{j,k}^\rho \equiv \left\langle \left\{ \hat{x}_j - \mu_j^\rho, \hat{x}_k - \mu_k^\rho \right\} \right\rangle^\rho. \tag{11}$$

A $2m \times 2m$ matrix S is symplectic if it preserves the symplectic form: $S\Omega S^T = \Omega$. According to Williamson's theorem [40], there is a diagonalization of the covariance matrix V^ρ of the form,

$$V^\rho = S^\rho \left(D^\rho \oplus D^\rho \right) \left(S^\rho \right)^T, \tag{12}$$

where S^ρ is a symplectic matrix and $D^\rho \equiv \operatorname{diag}(\nu_1, \ldots, \nu_m)$ is a diagonal matrix of symplectic eigenvalues such that $\nu_i \geq 1$ for all $i \in \{1, \ldots, m\}$. We say that a quantum Gaussian state is faithful if all of its symplectic eigenvalues are strictly greater than one (this also means that the state is positive definite). We can write the density operator ρ of a faithful state in the following exponential form [41–43] (see also [1, 34]):

$$\rho = (Z^\rho)^{-1/2} \exp\left[-\frac{1}{2} (\hat{x} - \mu^\rho)^T G^\rho (\hat{x} - \mu^\rho) \right], \tag{13}$$

$$\text{with} \quad Z^\rho \equiv \det([V^\rho + i\Omega]/2) \tag{14}$$

$$\text{and} \quad G^\rho \equiv -2\Omega S^\rho \left[\operatorname{arcoth}(D^\rho) \right]^{\oplus 2} \left(S^\rho \right)^T \Omega, \tag{15}$$

where $\operatorname{arcoth}(x) \equiv \frac{1}{2} \ln\left(\frac{x+1}{x-1} \right)$ with domain $(-\infty, -1) \cup (1, +\infty)$. Note that we can also write

$$G^\rho = 2i\Omega \operatorname{arcoth}(iV^\rho \Omega), \tag{16}$$

so that G^ρ is represented directly in terms of the covariance matrix V^ρ. Faithfulness of Gaussian states is required to ensure that G^ρ is non-singular. By inspection, the G and V matrices are symmetric. In what follows, we adopt the same notation for quantities associated with a density operator σ, such as μ^σ, V^σ, S^σ, D^σ, Z^σ, and G^σ.

A two-mode Gaussian state ρ with covariance matrix in "standard form" has a covariance matrix as follows [44, 45]:

$$V^\rho = \begin{bmatrix} a & c \\ c & b \end{bmatrix} \oplus \begin{bmatrix} a & -c \\ -c & b \end{bmatrix}. \tag{17}$$

The symplectic diagonalization of the covariance matrix V simplifies as well [46]:

$$V = S \left(D \oplus D \right) S^T, \tag{18}$$

where

$$S = \left(I_2 \oplus \sigma_Z \right) S_0^{\oplus 2} \left(I_2 \oplus \sigma_Z \right), \tag{19}$$

$$S_0 = \begin{bmatrix} \omega_+ & \omega_- \\ \omega_- & \omega_+ \end{bmatrix}, \qquad \omega_\pm = \sqrt{\frac{a + b \pm \sqrt{y}}{2\sqrt{y}}}, \tag{20}$$

$$D = \begin{bmatrix} \nu_- & 0 \\ 0 & \nu_+ \end{bmatrix}, \qquad \nu_\pm = \left[\sqrt{y} \pm (b - a) \right]/2, \tag{21}$$

$$y = (a + b)^2 - 4c^2, \tag{22}$$

and σ_Z denotes the standard Pauli Z matrix. Given a two-mode state with covariance matrix in standard form as in (17), it is a separable state if and only if

$$c \leq c_{\text{sep}} \equiv \sqrt{(a - 1)(b - 1)}, \tag{23}$$

which can be determined from the condition given in [47, Eq. (14)]. We return to this condition when we discuss the relative entropy of entanglement for quantum Gaussian states.

A quantum Gaussian channel is one that preserves Gaussian states [33, 34, 48]. The action of a quantum Gaussian channel on an input state ρ is characterized by two matrices X and Y, which transform the covariance matrix V^ρ of ρ as follows:

$$V^\rho \to X V^\rho X^T + Y, \tag{24}$$

where X^T is the transpose of the matrix X. In this formalism, the thermal channel $\mathcal{L}_{\eta, N_B}$ with transmissivity $\eta \in (0, 1)$ and thermal mean photon number $N_B > 0$ is given by

$$X = \sqrt{\eta} I_2, \qquad Y = (1 - \eta)(2N_B + 1) I_2, \tag{25}$$

where I_2 is the 2×2 identity matrix. Our principal focus in this paper is on the thermal channel.

B. Teleportation simulation and reduction by teleportation

Teleportation simulation of a channel [35–39] is a key tool used to establish the upper bounds in (1), (2), (6), and (8). The basic idea behind this tool is that channels with sufficient symmetry can be simulated by the action of a teleportation protocol [49–51] on a resource

state ω_{AB} shared between the sender A and receiver B. More generally, a channel $\mathcal{N}_{A'\to B}$ with input system A' and output system B is defined to be teleportation simulable with associated resource state ω_{AB} if the following equality holds for all input states $\rho_{A'}$ [36, Eq. (11)]:

$$\mathcal{N}_{A'\to B}(\rho_{A'}) = \mathcal{T}_{A'AB}(\rho_{A'} \otimes \omega_{AB}), \tag{26}$$

where $\mathcal{T}_{A'AB}$ is a quantum channel consisting of local operations and classical communication between the sender, who has systems A' and A, and the receiver, who has system B ($\mathcal{T}_{A'AB}$ can also be considered a generalized teleportation protocol, as in [51]). The implication of channel simulation via teleportation is that the performance of a general protocol that uses the channel n times, with each use interleaved by local operations and classical communication (LOCC), can be bounded from above by the performance of a protocol with a much simpler form: the simplified protocol consists of a single round of LOCC acting on n copies of ω_{AB} [35, 38, 39]. This is called reduction by teleportation. Of course, a secret-key-agreement protocol is one particular kind of protocol of the above form, as considered in [9, 13], and so the general reduction method of [35, 38, 39] applies.

For continuous-variable bosonic systems, the teleportation simulation of a single-mode bosonic Gaussian channels was considered in [38], and the simulation therein only simulates the channel exactly in the limit in which the resource state is the result of transmitting one share of an infinitely-squeezed, two-mode squeezed vacuum state [34] through the channel (this resource state is sometimes called the Choi state of the channel [34], and we use this terminology in what follows). Thus, when applying this argument to bound the rates of secret-key-agreement protocols as discussed above, one must take care with an appropriate limiting argument, as pointed out in [53] and handled already in [13]. This teleportation simulation argument with an infinitely-squeezed resource state is one of the core steps used to establish the bounds in (1), (2), (6), and (8).

Recently, an important development in the theory of the teleportation simulation of quantum Gaussian channels has taken place [26]. In particular, the authors of [26] have shown that all single-mode, phase-insensitive quantum Gaussian channels other than the pure-loss channel can be simulated via the action of teleportation on a finite-energy Gaussian resource state that has the same amount of entanglement as the Choi state of the channel. In [26], the authors quantified the amount of entanglement in the resource state using an entanglement monotone [54] called logarithmic negativity, which is the same entanglement measure considered in [38]. In our paper, we show how the main idea of their paper leads to strengthened bounds on the performance of secret-key-agreement protocols conducted over single-mode phase-insensitive bosonic Gaussian channels.

To describe the result of [26] in more detail, let $X = \sqrt{\tau} I_2$ and $Y = y I_2$ be the matrices representing the action of a single-mode phase-insensitive Gaussian channel on an input state, as in (24). In what follows and as in [26], we exclusively consider the case when $\tau \geq 0$. In order for the map to be a completely positive, trace-preserving map (i.e., a legitimate quantum channel), the following inequality should hold [34]

$$y \geq |1 - \tau| . \tag{27}$$

The main contribution of [26] is that every single-mode phase-insensitive Gaussian channel in the above class, besides the pure-loss channel, can be simulated by the action of a continuous-variable teleportation protocol on a finite-energy, two-mode resource state with the same amount of entanglement as the Choi state of the channel. An additional contribution of [26] is a converse bound: it is not possible to use a resource state with logarithmic negativity smaller than that of the Choi state, in order to simulate the channel. This follows directly from the facts that the teleportation simulation protocol should simulate the channel, teleportation is an LOCC, and logarithmic negativity is an entanglement monotone (it is non-increasing with respect to an LOCC). This converse bound holds, by the same argument, for all measures of entanglement (such as relative entropy of entanglement).

In more detail, the teleportation simulation of [26] begins with the sender and receiver of the channel sharing a two-mode Gaussian state in the standard form in (17). The sender mixes the input of the channel and her share of the resource state on a 50-50 beam splitter. The sender then performs ideal homodyne detection of the position quadrature of the first mode and ideal homodyne detection of the momentum quadrature of the second mode, leading to measurement outcomes Q_+ and P_-. The sender communicates these real values over ideal classical communication channels to the receiver, and the receiver performs displacement operations of his mode by $g\sqrt{2}Q_+$ and $g\sqrt{2}P_-$, for some $g \in \mathbb{R}$. The result of all of these operations is to implement a quantum Gaussian channel of the following form on the input state:

$$X = g I_2, \tag{28}$$

$$Y = \left[g^2 a + 2gc + b\right] I_2, \tag{29}$$

where we note the different sign convention from [26, Eq. (7)], due to our slightly different convention for the standard form in (17). If $g > 0$, then the channel implemented is a single-mode phase-insensitive Gaussian channel with

$$\tau = g^2, \qquad y = g^2 a + 2gc + b. \tag{30}$$

If $g < 0$, then one can postprocess the output according to a unitary Gaussian channel with $X = -I_2$ and $Y = 0$ (a phase flip channel), such that the overall channel is a single-mode phase-insensitive Gaussian channel with τ and y as in (30). A generalization of these steps beyond two-mode states is given in [37].

Where [26] departs from prior works is to solve an inverse problem regarding teleportation simulation. Given

values of τ and y corresponding to a physical channel different from the pure-loss channel, the authors of [26] proved that there exists a finite-energy, two-mode Gaussian state in standard form satisfying (30), having its smaller symplectic eigenvalue equal to one, and having its logarithmic negativity equal to that of the Choi state of the channel. It should be stressed that the states found in [26] have an analytical form, which has to do with the form of the above constraints.

C. Information quantities and bounds for secret-key-agreement protocols

The basic information quantities that we need in this paper are the quantum relative entropy [55, 56], the relative entropy variance [57, 58], and the hypothesis testing relative entropy [20, 59]. For two states ρ and σ defined on a separable Hilbert space with the following spectral decompositions:

$$\rho = \sum_x \lambda_x |\phi_x\rangle\langle\phi_x|, \tag{31}$$

$$\sigma = \sum_y \mu_y |\psi_y\rangle\langle\psi_y|, \tag{32}$$

the quantum relative entropy $D(\rho\|\sigma)$ [56] and the relative entropy variance $V(\rho\|\sigma)$ [57, 58] are defined as

$$D(\rho\|\sigma) = \sum_{x,y} |\langle\psi_y|\phi_x\rangle|^2 \lambda_x \log_2(\lambda_x/\mu_y), \tag{33}$$

$$V(\rho\|\sigma) = \sum_{x,y} |\langle\psi_y|\phi_x\rangle|^2 \lambda_x \left[\log_2(\lambda_x/\mu_y) - D(\rho\|\sigma)\right]^2. \tag{34}$$

For quantum Gaussian states, the quantities $D(\rho\|\sigma)$ [41], [9] and $V(\rho\|\sigma)$ [60] can be expressed in terms of their first and second moments. For simplicity, let us suppose that ρ and σ are zero-mean quantum Gaussian states. Then Refs. [41], [9] established that

$$D(\rho\|\sigma) = \log_2(Z^\sigma/Z^\rho)/2 - \mathrm{Tr}\{\Delta V^\rho\}/4\ln 2, \tag{35}$$

where $\Delta = G^\rho - G^\sigma$, and Ref. [60] established that

$$V(\rho\|\sigma) = \frac{1}{8\ln^2 2}\left[\mathrm{Tr}\{\Delta V^\rho \Delta V^\rho\} + \mathrm{Tr}\{\Delta\Omega\Delta\Omega\}\right]. \tag{36}$$

In the above, we should note that our convention for normalization of covariance matrices is what leads to the different constant prefactors when compared to the expressions in [9, 41, 60].

The hypothesis testing relative entropy is defined as [20, 59]

$$D_H^\varepsilon(\rho\|\sigma) = -\log_2 \inf_\Lambda \{\mathrm{Tr}\{\Lambda\sigma\} : 0 \leq \Lambda \leq I \wedge \mathrm{Tr}\{\Lambda\rho\} \geq 1-\varepsilon\} \tag{37}$$

By the reasoning in [61] and Appendix C, we have the following bound holding for faithful states ρ and σ such that $D(\rho\|\sigma), V(\rho\|\sigma), T(\rho\|\sigma) < \infty$ and $V(\rho\|\sigma) > 0$:

$$D_H^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) \leq nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\Phi^{-1}(\varepsilon) + O(\log n), \tag{38}$$

where [57, 58]

$$T(\rho\|\sigma) = \sum_{x,y} |\langle\psi_y|\phi_x\rangle|^2 \lambda_x \left|\log_2(\lambda_x/\mu_y) - D(\rho\|\sigma)\right|^3, \tag{39}$$

and

$$\Phi(a) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^a dx\ \exp\left(\frac{-x^2}{2}\right) \tag{40}$$

$$\Phi^{-1}(\varepsilon) = \sup\{a \in \mathbb{R} \mid \Phi(a) \leq \varepsilon\}. \tag{41}$$

We note here that the finiteness of $T(\rho\|\sigma)$ for finite-energy, faithful Gaussian states is essential to the main result of our paper. Inspecting the proof given in Appendix C, we see that the condition $T(\rho\|\sigma) < \infty$ allows us to invoke the Berry-Esseen theorem [27, 28], which in turn leads to the improved upper bound in (9).

The relative entropy of entanglement of a bipartite state ρ_{AB} is defined as follows [62]:

$$E_R(A;B)_\rho = \inf_{\sigma_{AB}\in \mathrm{SEP}(A:B)} D(\rho_{AB}\|\sigma_{AB}), \tag{42}$$

where $\mathrm{SEP}(A:B)$ denotes the set of separable (unentangled) states [63]. Analogously, we have the ε-relative entropy of entanglement [64]:

$$E_R^\varepsilon(A;B)_\rho = \inf_{\sigma_{AB}\in \mathrm{SEP}(A:B)} D_H^\varepsilon(\rho_{AB}\|\sigma_{AB}). \tag{43}$$

For a two-mode Gaussian state ρ_{AB} in standard form, one can always choose the separable state σ'_{AB} to be in standard form with the same values for a and b but with c chosen to saturate the inequality in (23), such that $c = c_{\mathrm{sep}}$ [9]. By definition, for this suboptimal choice, we have that

$$E_R(A;B)_\rho \leq D(\rho_{AB}\|\sigma'_{AB}), \tag{44}$$

$$E_R^\varepsilon(A;B)_\rho \leq D_H^\varepsilon(\rho_{AB}\|\sigma'_{AB}), \tag{45}$$

and this is the choice made in [9, 13] to arrive at various upper bounds on secret-key-agreement capacity. In what follows, we refer to $D(\rho_{AB}\|\sigma'_{AB})$ as the suboptimal relative entropy of entanglement of ρ_{AB}.

In [13, Eq. (4.34)], the following bound was established on the non-asymptotic secret-key-agreement capacity of a channel $\mathcal{N}$ that is teleportation simulable with associated resource state ω_{AB}:

$$P_{\mathcal{N}}^{\leftrightarrow}(n,\varepsilon) \leq \frac{1}{n}E_R^\varepsilon(A^n;B^n)_{\omega^{\otimes n}} \leq \frac{1}{n}D_H^\varepsilon(\omega_{AB}^{\otimes n}\|\sigma_{AB}^{\otimes n}). \tag{46}$$

The argument for the first inequality critically relies upon the connection between secret-key-agreement protocols

and private-state distillation protocols established in [65, 66] and some other results contained therein, in addition to the teleportation reduction argument discussed in Section II B. The second inequality follows from the definition in (43), with σ_{AB} being an arbitrary separable state. Thus, any resource state for the teleportation simulation of a channel can be used to give an upper bound on its non-asymptotic secret-key-agreement capacity. In particular, if ω_{AB} and σ_{AB} are faithful quantum Gaussian states of finite energy such that $\omega_{AB} \neq \sigma_{AB}$, then the conditions $D(\omega_{AB}\|\sigma_{AB}), V(\omega_{AB}\|\sigma_{AB}), T(\omega_{AB}\|\sigma_{AB}) < \infty$ and $V(\omega_{AB}\|\sigma_{AB}) > 0$ hold, such that (38) applies and we find that

$$P_{\mathcal{N}}^{\leftrightarrow}(n,\varepsilon) \leq D(\omega_{AB}\|\sigma_{AB}) + \sqrt{\frac{V(\omega_{AB}\|\sigma_{AB})}{n}}\Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right). \quad (47)$$

The quantities $D(\omega_{AB}\|\sigma_{AB})$ and $V(\omega_{AB}\|\sigma_{AB})$ are finite for faithful quantum Gaussian states of finite energy, which holds by inspecting (35) and (36), and in Appendix D, we argue that the quantity $T(\omega_{AB}\|\sigma_{AB})$ is finite as well.

Note that both (6) and (9) can be derived from (46). The point of deviation in the two derivations is that it is possible, on the one hand, to invoke the Berry–Esseen theorem [27, 28] in order to arrive at (9), due to the results of [26] and our arguments in Appendices C and D. That is, [26] showed how to perform teleportation simulation of a single-mode phase-insensitive thermal bosonic channel using a finite-energy resource state, and our Appendix D argues how $T(\omega_{AB}\|\sigma_{AB})$ is finite for finite-energy Gaussian states. Thus, the Berry–Esseen theorem can be invoked as shown in Appendix C and so (38) applies. On the other hand, for the derivation of (6), the ideal infinite-energy Choi state of the channel is used as the resource state, but it is not known if $T(\omega_{AB}\|\sigma_{AB})$ is finite in such a scenario. Hence, unless this is proven, we cannot invoke (38). Therefore, other techniques, such as the Chebyshev inequality, were used in [13] to arrive at (6).

III. METHODS

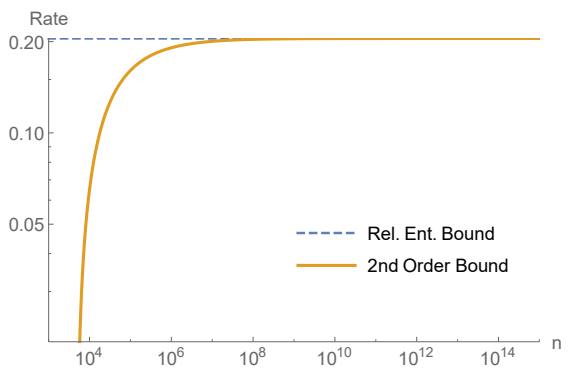
Given the background reviewed above, we are now in a position to discuss the main contribution of our paper. We modify the finite-energy teleportation simulation approach of [26] in the following way: Given a thermal channel with $\tau = \eta$ and $y = (1-\eta)(2N_B+1)$, we find a finite-energy, two-mode Gaussian state in standard form such that

1. it satisfies (30),
2. its smaller symplectic eigenvalue is just larger than one, and
3. its suboptimal relative entropy of entanglement is equal to the suboptimal relative entropy of entanglement of the Choi state of the channel, the latter of which is given by (4).

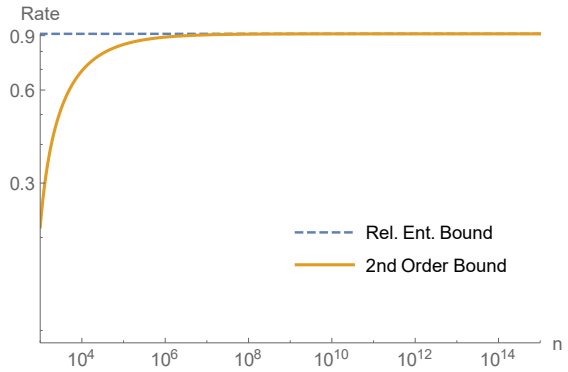
Any resource state that simulates the channel should satisfy the first constraint. We impose the second constraint to ensure that the state we find is a faithful Gaussian state, such that its relative entropy and relative entropy variance to a separable Gaussian state can be easily evaluated using the formulas in (35) and (36). As discussed above, the relative entropy of entanglement of the resource state should at least be equal to that of the Choi state, in order to simulate a channel. In order to ensure that we find a good upper bound on the secret-key-agreement capacity, we have imposed the third constraint on suboptimal relative entropy of entanglement. We find these states by numerically solving the above constraints with the aid of a computer program [67], and we remark that finding an analytical solution in this case appears to be far more complicated than for the case from [26], due to the fact that the suboptimal relative entropy of entanglement is a much more complicated function of the covariance matrix elements. In some cases, it is possible to find multiple solutions for the states that satisfy these constraints. For our purpose, any of these states can be chosen. We also note that the flexibility afforded by having a teleportation simulation with negative gain g, as discussed in Section II B, is critical for us to solve these constraints by numerical search. With these finite-energy states in hand, we then numerically compute the relative entropy variance in (36) and can apply the bound in (47).

IV. RESULTS

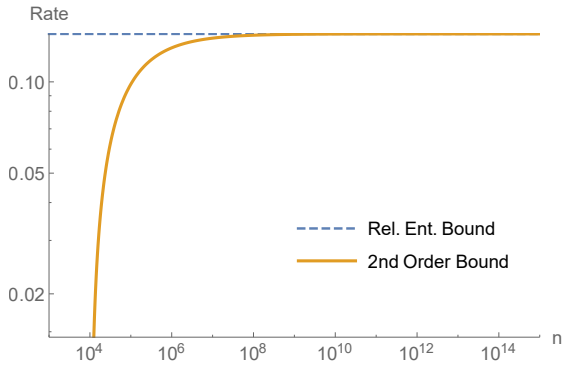
In Figure 1, we plot upper bounds on the asymptotic secret-key-agreement capacity of the thermal channel given by (4) (dashed line) and upper bounds on the non-asymptotic secret-key-agreement capacity given by (9) (solid line) versus the number of channel uses. It is important to stress that the latter bound is only an approximation (known as the normal approximation) if n is not sufficiently large (i.e., n should be proportional to $1/\varepsilon^2$ in order for the bounds to really apply). At the same time, many prior works have shown that the normal approximation is an excellent approximation for non-asymptotic capacities even for small n [21, 29–32]. In each case, we choose the key-quality parameter ε to be 10^{-10}, in accordance with the same conservative value chosen in [68]. In the plots, we select $\eta \in (0,1)$, (hence the corresponding distance L) and the thermal mean photon number $N_B > 0$ as indicated above each figure. The distance L can be related to the transmissivity η of the thermal channel as $\eta = \exp[-L/L_0]$, where L_0 is the fiber attenuation length [17]. In the plots, we consider $L_0 = 22$ km. The thermal mean photon number N_B relevant in experimental contexts, whenever thermal



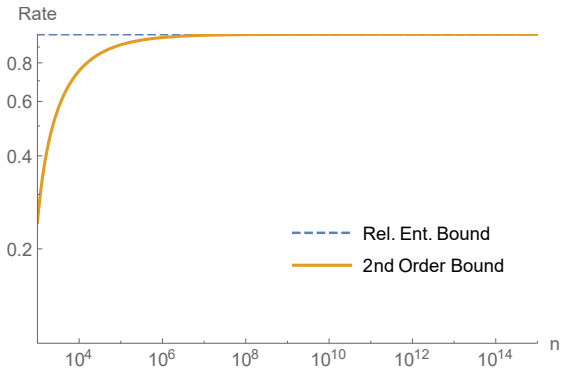
(a) $N_B = 0.1$, $L = 26.49\,\text{km}$, $\eta = 0.3$



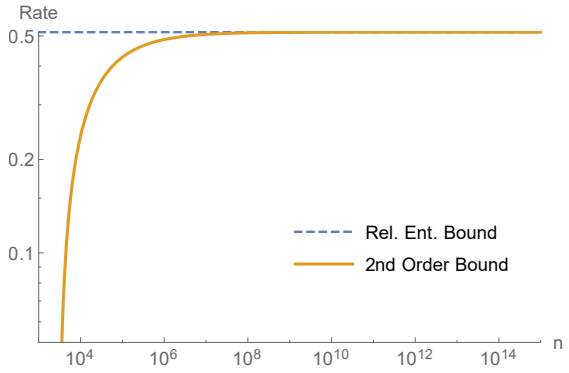
(b) $N_B = 0.1$, $L = 11.23\,\text{km}$, $\eta = 0.6$



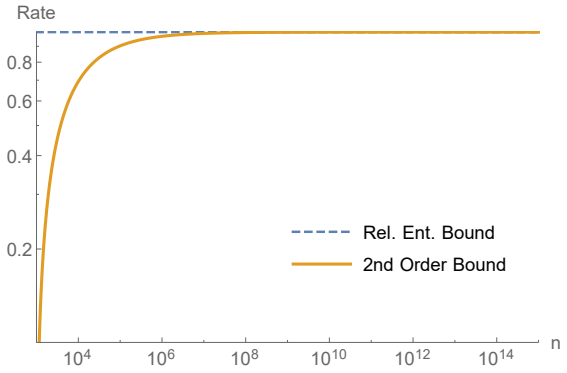
(c) $N_B = 10^{-3}$, $L = 50.65\,\text{km}$, $\eta = 0.1$



(d) $N_B = 10^{-3}$, $L = 15.25\,\text{km}$, $\eta = 0.5$



(e) $N_B = 3 \times 10^{-7}$, $L = 26.49\,\text{km}$, $\eta = 0.3$



(f) $N_B = 3 \times 10^{-7}$, $L = 15.25\,\text{km}$, $\eta = 0.5$

FIG. 1. The figures plot upper bounds on the non-asymptotic secret-key-agreement capacity of the thermal channels of transmissivity $\eta \in (0, 1)$ and thermal mean photon number $N_B > 0$ given by the second-order approximation from (9). In each figure, we select certain values of η (corresponding to a certain distance L via $\eta = \exp[-L/L_0]$) and N_B, as indicated below each figure. In all cases, we take the conservative value of $\varepsilon = 10^{-10}$ as indicated in [68]. Each figure indicates that the asymptotic secret-key-agreement capacity is too pessimistic of a benchmark for demonstrating a quantum repeater when using the channel a finite number of times. That is, there is an appreciable difference between the asymptotic and non-asymptotic secret-key-agreement capacity.

noise is due exclusively to dark counts, is given by the dark counts per second times the integration period t_{int}. In the plots, the lowest N_B we consider corresponds to a dark count rate of 10 per second and $t_{\text{int}} = 30$ ns [17, Section VI]. For completeness, we also consider higher values of N_B, which could occur due to excessive background thermal radiation or tampering by an eavesdropper.

As noted in the introduction of our paper, these upper bounds can be interpreted to serve as benchmarks for quantum repeaters [19]. That is, the upper bounds

on secret-key-agreement capacity hold for any protocol that uses the channel and LOCC but is not allowed to use a quantum repeater. As such, exceeding these upper bounds constitutes a demonstration of a quantum repeater [19]. What our results indicate is that the previous upper bounds from [9, 13] on the asymptotic secret-key-agreement capacity are too pessimistic of a benchmark for protocols that are only using the channel a finite number of times. As such, the burden of demonstrating a quantum repeater is now somewhat relieved in comparison to what was previously thought would be necessary.

From an experimental perspective, it could be of interest to perform a test using the results of our paper in order to demonstrate a working quantum repeater. A convincing approach for doing so would be to conduct an actual secret-key-distillation protocol over some finite number of uses of the channel and determine what secret-key rates can be achieved. [17, Section IV] details methods for determining secret-key rates that are achievable in particular physical setups. For a given rate and number of channel uses, one can then compare the results with our plots (or other plots generated via the same method for different parameter values) to determine if the rate is achieved is larger than the upper bounds in our plots; if it is the case, then one can claim a working quantum repeater, albeit with the understanding that our upper bounds are the normal approximations of the true finite-length upper bounds (as discussed previously). This approach is to be contrasted with those that estimate the quantum bit-error rate from just a few channel uses and then use this parameter to calculate an asymptotic key rate (see the review in [69] for discussions of such approaches).

V. CONCLUSION

In this paper, we showed how to extend the teleportation simulation method of [26] to the relative entropy of entanglement measure. By combining with prior results in [13] regarding non-asymptotic secret-key-agreement capacity, this extension leads to improved bounds on the non-asymptotic secret-key-agreement capacity of a thermal bosonic channel, in certain parameter regimes. Given that upper bounds on secret-key-agreement capacity have been advocated as a way to assess the performance of a quantum repeater, our results indicate that previous bounds from [9, 13] are too pessimistic, and it should be somewhat easier to demonstrate a working quantum repeater in the realistic regime of a finite number of channel uses.

We remark that our approach can be extended to quantum amplifier channels, but we did not discuss these channels in any detail because they appear to be most prominently physically relevant in exotic relativistic communication scenarios [70–72]. Our approach also applies to single-mode additive-noise Gaussian channels.

Going forward from here, it would be interesting to generalize our results to multimode bosonic communication channels [48] or channels that are not phase-insensitive. As discussed previously [11, 13, 18], it would also be good to determine bounds on performance when there is an average energy constraint at the input of each channel use. One should expect to find improved upper bounds due to this extra constraint.

Note: After our paper appeared on the arXiv, we became aware of a preprint [73] with related results.

ACKNOWLEDGMENTS

We are grateful to Gerardo Adesso, Boulat Bash, Mario Berta, Zachary Dutton, Jens Eisert, Saikat Guha, Jonathan P. Dowling, Jeffrey H. Shapiro, and Marco Tomamichel for discussions. We also thank the anonymous referees for their constructive comments that helped to improve our paper. We acknowledge support from the Office of Naval Research.

Appendix A: Little room for improving the strong converse bound in (1)

Here we argue why we think it will not be possible to improve upon the upper bound in (1), up to lower-order terms. Before proceeding, recall that the conditional quantum entropy and conditional entropy variance [58] are defined for a bipartite state ρ_{AB} as

$$H(A|B)_\rho \equiv -D(\rho_{AB}\|I_A \otimes \rho_B), \tag{A1}$$
$$V(A|B)_\rho \equiv V(\rho_{AB}\|I_A \otimes \rho_B). \tag{A2}$$

The coherent information is defined as $I(A\rangle B)_\rho \equiv -H(A|B)_\rho$ [74] and its corresponding variance is $V(A\rangle B)_\rho \equiv V(A|B)_\rho$. In [13, Section 6.2], the following achievability bound was established for $\mathcal{N}$ a finite-dimensional channel:

$$P^{\leftrightarrow}_{\mathcal{N}}(n,\varepsilon) \geq I_{\text{rev}}(\mathcal{N}) + \sqrt{\frac{V^{\varepsilon}_{\text{rev}}(\mathcal{N})}{n}}\Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right) \tag{A3}$$

where $I_{\text{rev}}(\mathcal{N})$ is the following quantity [75, Section 5.3] (sometimes called the channel's reverse coherent information):

$$I_{\text{rev}}(\mathcal{N}) \equiv \max_{|\psi\rangle_{AA'} \in \mathcal{H}_{AA'}} I(B\rangle A)_\theta, \tag{A4}$$

$\theta_{AB} \equiv \mathcal{N}_{A'\to B}(\psi_{AA'})$, and $V^{\varepsilon}_{\text{rev}}(\mathcal{N})$ is the channel's reverse conditional entropy variance:

$$V^{\varepsilon}_{\text{rev}}(\mathcal{N}) \equiv \begin{cases} \min_{\psi_{AA'} \in \Pi_{\text{rev}}} V(B\rangle A)_\theta & \text{for } \varepsilon < 1/2 \\ \max_{\psi_{AA'} \in \Pi_{\text{rev}}} V(B\rangle A)_\theta & \text{for } \varepsilon \geq 1/2 \end{cases}. \tag{A5}$$

The set $\Pi_{\text{rev}} \subseteq \mathcal{D}(\mathcal{H}_{AA'})$ is the set of all states achieving the maximum in (A4).

The inequality in (A3) follows from a one-shot coding theorem [13, Proposition 21], followed by an expansion of the hypothesis testing relative entropy as [57, 58]

$$D_H^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) \geq nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\Phi^{-1}(\varepsilon) + O(\log n). \quad \text{(A6)}$$

A critical step employed in the above expansion is the Berry–Esseen theorem [27, 28]. Rather than employing the Berry–Esseen theorem, we can modify the proof of Theorem 2 in [57] (therein instead picking $L_n = \exp(nD(\rho\|\sigma) - \sqrt{nV(\rho\|\sigma)/\varepsilon})$) to employ the Chebyshev inequality and instead find the following expansion:

$$D_H^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) \geq nD(\rho\|\sigma) - \sqrt{\frac{nV(\rho\|\sigma)}{\varepsilon}}. \quad \text{(A7)}$$

For these theorems to hold in separable infinite-dimensional Hilbert spaces, it remains to show how to connect the coding theorem in [13, Proposition 21] to the inequality in (A7), but we strongly suspect that this should be possible. If everything holds, we would obtain the following achievability theorem for an infinite-dimensional channel $\mathcal{N}$:

$$P_{\mathcal{N}}^{\leftrightarrow}(n,\varepsilon) \geq I_{\text{rev}}(\mathcal{N}) - \sqrt{\frac{V_{\text{rev}}^\varepsilon(\mathcal{N})}{n\varepsilon}} + O\left(\frac{1}{n}\right). \quad \text{(A8)}$$

The above would hold for all finite-energy two-mode, squeezed vacuum states passed through the channel, and one could then take a limit as the photon number approaches infinity. The term $I_{\text{rev}}(\mathcal{N})$ converges to $-\log_2(1-\eta)$ [9]. Below we show that the relative entropy variance $V_{\text{rev}}^\varepsilon(\mathcal{N})$ term converges to zero. This would then give the following bound

$$P_{\mathcal{L}_\eta}^{\leftrightarrow}(n,\varepsilon) \geq -\log_2(1-\eta) + O\left(\frac{1}{n}\right), \quad \text{(A9)}$$

leading us to our conclusion that there is little room for improving the upper bound in (1). We stress that this remains to be worked out in detail.

We now evaluate the variance for the reverse coherent information when sending in a two-mode squeezed vacuum to a pure-loss channel of transmissivity $\eta \in (0,1)$. Recall that the quantity of interest is

$$\begin{aligned}
&V(B\rangle A) \\
&= \text{Tr}\{\rho_{AB}\left[\log\rho_{AB} - \log\rho_A\right]^2\} && \text{(A10)}\\
&\quad - \left[H(AB)_\rho - H(A)_\rho\right]^2 && \text{(A11)}\\
&= \text{Tr}\{\rho_{AB}\left[\log\rho_{AB}\right]^2\} \\
&\quad - 2\,\text{Tr}\{\rho_{AB}\log\rho_{AB}\log\rho_A\} + \text{Tr}\{\rho_{AB}\left[\log\rho_A\right]^2\} \\
&\quad - \left[H(AB)_\rho - H(A)_\rho\right]^2 && \text{(A12)}\\
&= \text{Tr}\{\rho_{AB}\left[\log\rho_{AB}\right]^2\} - H(AB)_\rho^2 \\
&\quad - 2\left[\text{Tr}\{\rho_{AB}\log\rho_{AB}\log\rho_A\} - H(A)_\rho H(AB)_\rho\right] \\
&\quad + \text{Tr}\{\rho_A\left[\log\rho_A\right]^2\} - H(A)_\rho^2. && \text{(A13)}
\end{aligned}$$

The first and last terms we can evaluate easily using the following formula for the entropy variance of a thermal state with mean photon number N_S [76, Appendix A]:

$$V(N_S) = N_S\left(N_S+1\right)\left[\log\left(1+\frac{1}{N_S}\right)\right]^2. \quad \text{(A14)}$$

For the first, using the notion of purification, purifying with ψ_{ABE}, and observing that ψ_E is a thermal state with mean photon number $(1-\eta)N_S$, we find that

$$\begin{aligned}
&\text{Tr}\{\rho_{AB}\left[\log\rho_{AB}\right]^2\} - H(AB)_\rho^2 \\
&= \text{Tr}\{\psi_E\left[\log\psi_E\right]^2\} - H(E)_\psi^2 && \text{(A15)}\\
&= (1-\eta)N_S\left((1-\eta)N_S+1\right)\left[\log\left(1+\frac{1}{(1-\eta)N_S}\right)\right]^2. && \text{(A16)}
\end{aligned}$$

For the last term, we observe that ρ_A is a thermal state with mean photon number N_S, which implies that

$$\begin{aligned}
&\text{Tr}\{\rho_A\left[\log\rho_A\right]^2\} - H(A)_\rho^2 \\
&\qquad = N_S\left(N_S+1\right)\left[\log\left(1+\frac{1}{N_S}\right)\right]^2. && \text{(A17)}
\end{aligned}$$

So it remains to handle the middle term. Consider that

$$\begin{aligned}
&\text{Tr}\{\rho_{AB}\log\rho_{AB}\log\rho_A\} \\
&= \text{Tr}\{\psi_{ABE}\log\rho_{AB}\log\rho_A\} && \text{(A18)}\\
&= \text{Tr}\{\psi_{ABE}\log\psi_E\log\rho_A\} && \text{(A19)}\\
&= \text{Tr}\{\psi_{AE}\log\psi_E\log\rho_A\}. && \text{(A20)}
\end{aligned}$$

Consider that we can write

$$\psi_E = \left[(1-\eta)N_S+1\right]^{-1}\left(1+\frac{1}{(1-\eta)N_S}\right)^{-\hat{n}_E}, \quad \text{(A21)}$$

$$\rho_A = \left[N_S+1\right]^{-1}\left(1+\frac{1}{N_S}\right)^{-\hat{n}_A}, \quad \text{(A22)}$$

where $\hat{n}_E$ and $\hat{n}_A$ are the number operators. This means that

$$\begin{aligned}
&\text{Tr}\{\psi_{AE}\log\psi_E\log\rho_A\} \\
&= \text{Tr}\left\{\psi_{AE}\log\left[\left[(1-\eta)N_S+1\right]^{-1}\left(1+\frac{1}{(1-\eta)N_S}\right)^{-\hat{n}_E}\right]\right. \\
&\qquad \left.\times\log\left[\left[N_S+1\right]^{-1}\left(1+\frac{1}{N_S}\right)^{-\hat{n}_A}\right]\right\} && \text{(A23)}\\
&= \text{Tr}\left\{\psi_{AE}\log\left[\left[(1-\eta)N_S+1\right]\left(1+\frac{1}{(1-\eta)N_S}\right)^{\hat{n}_E}\right]\right. \\
&\qquad \left.\times\log\left[\left[N_S+1\right]\left(1+\frac{1}{N_S}\right)^{\hat{n}_A}\right]\right\} && \text{(A24)}
\end{aligned}$$

$$
\begin{aligned}
&= \log\left[(1-\eta)\,N_S+1\right]\log\left[N_S+1\right] \\
&+ \log\left[\left[(1-\eta)\,N_S+1\right]\right]\log\left[\left(1+\frac{1}{N_S}\right)\right]\mathrm{Tr}\left\{\psi_{AE}\hat{n}_A\right\} \\
&+ \log\left[1+\frac{1}{(1-\eta)\,N_S}\right]\log\left[N_S+1\right]\mathrm{Tr}\left\{\psi_{AE}\hat{n}_E\right\} \\
&+ \log\left[1+\frac{1}{(1-\eta)\,N_S}\right]\log\left[1+\frac{1}{N_S}\right]\mathrm{Tr}\left\{\psi_{AE}\left(\hat{n}_A\otimes\hat{n}_E\right)\right\}
\end{aligned} \tag{A25}
$$

$$
\begin{aligned}
&= \log\left[(1-\eta)\,N_S+1\right]\log\left[N_S+1\right] \\
&\quad + N_S\log\left[\left[(1-\eta)\,N_S+1\right]\right]\log\left[\left(1+\frac{1}{N_S}\right)\right] \\
&\quad + (1-\eta)\,N_S\log\left[1+\frac{1}{(1-\eta)\,N_S}\right]\log\left[N_S+1\right] \\
&\quad + \log\left[1+\frac{1}{(1-\eta)\,N_S}\right]\log\left[1+\frac{1}{N_S}\right]\times \\
&\qquad \mathrm{Tr}\left\{\psi_{AE}\left(\hat{n}_A\otimes\hat{n}_E\right)\right\}.
\end{aligned} \tag{A26}
$$

We note that the third equality follows by applying the identity $\log(ab^{\hat{x}}) = \log(a) + \hat{x}\log(b)$ for positive scalars a and b and a positive operator $\hat{x}$. So we need to evaluate the term $\mathrm{Tr}\left\{\psi_{AE}\left(\hat{n}_A\otimes\hat{n}_E\right)\right\}$. Consider that sending a number state $|n\rangle\langle n|$ through a beamsplitter of transmissivity $1-\eta$ leads to the following transformation:

$$
|n\rangle\langle n|_{A'} \to \sum_{k=0}^{n}\binom{n}{k}\left(1-\eta\right)^k\eta^{n-k}|k\rangle\langle k|_E. \tag{A27}
$$

The two-mode squeezed vacuum at the input has the following form:

$$
\frac{1}{\sqrt{N_S+1}}\sum_{n=0}^{\infty}\sqrt{\left(\frac{N_S}{N_S+1}\right)^n}|n\rangle_A|n\rangle_{A'}. \tag{A28}
$$

However since we are evaluating $\mathrm{Tr}\left\{\psi_{AE}\left(\hat{n}_A\otimes\hat{n}_E\right)\right\}$, and $\hat{n}_A$ and $\hat{n}_E$ are diagonal in the number basis, this is equivalent to the following:

$$
\begin{aligned}
&\frac{1}{N_S+1}\sum_{n=0}^{\infty}\sum_{k=0}^{n}\left(\frac{N_S}{N_S+1}\right)^n\binom{n}{k}\left(1-\eta\right)^k\eta^{n-k}\times \\
&\qquad \mathrm{Tr}\{\left(|n\rangle\langle n|_A\otimes|k\rangle\langle k|\right)\left(\hat{n}_A\otimes\hat{n}_E\right)\} \\
&= \frac{1}{N_S+1}\sum_{n=0}^{\infty}\sum_{k=0}^{n}\left(\frac{N_S}{N_S+1}\right)^n\binom{n}{k}\left(1-\eta\right)^k\eta^{n-k}nk
\end{aligned} \tag{A29}
$$

$$
= \frac{1}{N_S+1}\sum_{n=0}^{\infty}n\left(\frac{N_S}{N_S+1}\right)^n\sum_{k=0}^{n}\binom{n}{k}\left(1-\eta\right)^k\eta^{n-k}k. \tag{A30}
$$

Consider that the expression $\sum_{k=0}^{n}\binom{n}{k}\left(1-\eta\right)^k\eta^{n-k}k$ is equal to the mean of a binomial random variable with parameter $1-\eta$, and so

$$
\sum_{k=0}^{n}\binom{n}{k}\left(1-\eta\right)^k\eta^{n-k}k = n\left(1-\eta\right), \tag{A31}
$$

implying that the last line above is equal to

$$
\left(1-\eta\right)\frac{1}{N_S+1}\sum_{n=0}^{\infty}n^2\left(\frac{N_S}{N_S+1}\right)^n. \tag{A32}
$$

This is then equal to the second moment of a geometric random variable with parameter $p = 1/\left(N_S+1\right)$, so that

$$
\begin{aligned}
&\left(1-\eta\right)\frac{1}{N_S+1}\sum_{n=0}^{\infty}n^2\left(\frac{N_S}{N_S+1}\right)^n \\
&= \left(1-\eta\right)\left(N_S\left(N_S+1\right)+N_S^2\right) &\text{(A33)}\\
&= \left(1-\eta\right)N_S\left(2N_S+1\right). &\text{(A34)}
\end{aligned}
$$

Plugging into the above, we find the reduction

$$
\begin{aligned}
&= \log\left[(1-\eta)\,N_S+1\right]\log\left[N_S+1\right] \\
&\quad + N_S\log\left[\left[(1-\eta)\,N_S+1\right]\right]\log\left[\left(1+\frac{1}{N_S}\right)\right] \\
&\quad + (1-\eta)\,N_S\log\left[1+\frac{1}{(1-\eta)\,N_S}\right]\log\left[N_S+1\right] \\
&+ (1-\eta)\,N_S\left(2N_S+1\right)\log\left[1+\frac{1}{(1-\eta)\,N_S}\right]\log\left[1+\frac{1}{N_S}\right].
\end{aligned} \tag{A35}
$$

From this we should subtract the following quantity

$$
\begin{aligned}
&H(A)_\rho H(AB)_\rho \\
&= g(N_S)g((1-\eta)\,N_S) &\text{(A36)}\\
&= \left[\left(N_S+1\right)\log\left(N_S+1\right) - N_S\log N_S\right]\times \\
&\left[\begin{array}{c}\left((1-\eta)\,N_S+1\right)\log\left((1-\eta)\,N_S+1\right)\\ -(1-\eta)\,N_S\log\left(1-\eta\right)N_S\end{array}\right] &\text{(A37)}\\
&= \left[N_S\log\left(1+\frac{1}{N_S}\right)+\log\left(N_S+1\right)\right]\times \\
&\left[\left(1-\eta\right)N_S\log\left(1+\frac{1}{(1-\eta)\,N_S}\right)+\log\left(\left(1-\eta\right)N_S+1\right)\right] &\text{(A38)}
\end{aligned}
$$

$$
\begin{aligned}
&= \left(1-\eta\right)N_S^2\log\left(1+\frac{1}{N_S}\right)\log\left(1+\frac{1}{(1-\eta)\,N_S}\right) \\
&\quad + \left(1-\eta\right)N_S\log\left(N_S+1\right)\log\left(1+\frac{1}{(1-\eta)\,N_S}\right) \\
&\quad + N_S\log\left(1+\frac{1}{N_S}\right)\log\left(\left(1-\eta\right)N_S+1\right) \\
&\quad + \log\left(N_S+1\right)\log\left(\left(1-\eta\right)N_S+1\right),
\end{aligned} \tag{A39}
$$

leading to

$$\begin{aligned}
&\operatorname{Tr}\{\rho_{AB}\log\rho_{AB}\log\rho_A\} - H(A)_\rho H(AB)_\rho \\
&= (1-\eta)\,N_S\,(2N_S+1)\log\left[1+\frac{1}{(1-\eta)\,N_S}\right]\log\left[1+\frac{1}{N_S}\right] \\
&\quad - (1-\eta)\,N_S^2\log\left(1+\frac{1}{N_S}\right)\log\left(1+\frac{1}{(1-\eta)\,N_S}\right) \qquad \text{(A40)}\\
&= (1-\eta)\,N_S\,(N_S+1)\log\left[1+\frac{1}{(1-\eta)\,N_S}\right]\log\left[1+\frac{1}{N_S}\right]. \qquad \text{(A41)}
\end{aligned}$$

Putting everything together, we find that the variance of the reverse coherent information is given by

$$\begin{aligned}
&(1-\eta)\,N_S\,((1-\eta)\,N_S+1)\left[\log\left(1+\frac{1}{(1-\eta)\,N_S}\right)\right]^2 \\
&-2\,(1-\eta)\,N_S\,(N_S+1)\log\left[1+\frac{1}{(1-\eta)\,N_S}\right]\log\left[1+\frac{1}{N_S}\right] \\
&\quad + N_S\,(N_S+1)\left[\log\left(1+\frac{1}{N_S}\right)\right]^2. \qquad \text{(A42)}
\end{aligned}$$

For large N_S, we have that $((1-\eta)\,N_S+1)\approx(1-\eta)\,N_S$ and $(N_S+1)\approx N_S$, so that the above reduces to

$$\approx\left[(1-\eta)\,N_S\log\left(1+\frac{1}{(1-\eta)\,N_S}\right)-N_S\log\left(1+\frac{1}{N_S}\right)\right]^2, \qquad \text{(A43)}$$

which converges to zero as $N_S\to\infty$.

Appendix B: Weak converse bounds for secret-key-agreement capacities

Here we argue for the weak-converse bounds given in (2) and (8), and even more general weak-converse bounds. The weak-converse bounds are a direct consequence of the bounds in [13] and [20, Eq. (2)] (see also [21, Eq. (134)]).

First, recall from [20, Eq. (2)] and [21, Eq. (134)] that the following bound holds for hypothesis testing relative entropy for $\varepsilon\in(0,1)$:

$$D_H^\varepsilon(\rho\|\sigma)\leq\frac{1}{1-\varepsilon}\left[D(\rho\|\sigma)+h_2(\varepsilon)\right]. \qquad \text{(B1)}$$

To see this, consider that the definition of $D_H^\varepsilon(\rho\|\sigma)$ can be further constrained as

$$\begin{aligned}
&D_H^\varepsilon(\rho\|\sigma) = \\
&\quad -\log_2\inf_\Lambda\{\operatorname{Tr}\{\Lambda\sigma\}:0\leq\Lambda\leq I\wedge\operatorname{Tr}\{\Lambda\rho\}=1-\varepsilon\}. \qquad \text{(B2)}
\end{aligned}$$

That is, it suffices to optimize over measurement operators that meet the constraint $\operatorname{Tr}\{\Lambda\rho\}\geq 1-\varepsilon$ with equality. This follows because for any measurement operator Λ such that $\operatorname{Tr}\{\Lambda\rho\}>1-\varepsilon$, we can modify it by scaling it by a positive number $\lambda\in(0,1)$ such that $\operatorname{Tr}\{(\lambda\Lambda)\,\rho\}=1-\varepsilon$. The new operator $\lambda\Lambda$ is a legitimate measurement operator and the error probability $\operatorname{Tr}\{(\lambda\Lambda)\sigma\}$ only decreases under this scaling (i.e., $\operatorname{Tr}\{(\lambda\Lambda)\sigma\}<\operatorname{Tr}\{\Lambda\sigma\}$), which allows us to conclude (B2). Now for any measurement operator Λ such that $\operatorname{Tr}\{\Lambda\rho\}=1-\varepsilon$, the monotonicity of quantum relative entropy [77] with respect to quantum channels implies that

$$\begin{aligned}
&D(\rho\|\sigma) \\
&\geq D(\{1-\varepsilon,\varepsilon\}\|\{\operatorname{Tr}\{\Lambda\sigma\},1-\operatorname{Tr}\{\Lambda\sigma\}\}) \qquad \text{(B3)}\\
&= (1-\varepsilon)\log_2\left(\frac{1-\varepsilon}{\operatorname{Tr}\{\Lambda\sigma\}}\right)+\varepsilon\log_2\left(\frac{\varepsilon}{1-\operatorname{Tr}\{\Lambda\sigma\}}\right) \qquad \text{(B4)}\\
&= -(1-\varepsilon)\log_2\operatorname{Tr}\{\Lambda\sigma\}-h_2(\varepsilon) \\
&\qquad +\varepsilon\log_2\left(\frac{1}{1-\operatorname{Tr}\{\Lambda\sigma\}}\right) \qquad \text{(B5)}\\
&\geq -(1-\varepsilon)\log_2\operatorname{Tr}\{\Lambda\sigma\}-h_2(\varepsilon). \qquad \text{(B6)}
\end{aligned}$$

Rewriting this gives

$$-\log\operatorname{Tr}\{\Lambda\sigma\}\leq\frac{1}{1-\varepsilon}\left[D(\rho\|\sigma)+h_2(\varepsilon)\right]. \qquad \text{(B7)}$$

Since this bound holds for all measurement operators Λ satisfying $\operatorname{Tr}\{\Lambda\rho\}=1-\varepsilon$, we can conclude (B1).

To conclude the desired weak-converse bounds, we then invoke the above and [13, Eq. (4.34)] to get that the following bound holds for any teleportation simulable channel with associated resource state ω_{AB}:

$$\begin{aligned}
P_{\mathcal{N}}^{\leftrightarrow}(n,\varepsilon)&\leq\frac{1}{n}E_R^\varepsilon(A^n;B^n)_{\omega^{\otimes n}} \qquad \text{(B8)}\\
&\leq\frac{1}{n(1-\varepsilon)}\left[E_R(A^n;B^n)_{\omega^{\otimes n}}+h_2(\varepsilon)\right] \qquad \text{(B9)}\\
&\leq\frac{1}{(1-\varepsilon)}\left[E_R(A;B)_\omega+\frac{h_2(\varepsilon)}{n}\right]. \qquad \text{(B10)}
\end{aligned}$$

If the channel requires an infinite-energy resource state to become teleportation simulable, then one must take care as in the case of the proofs in [13, Section 8], and then one finally arrives at the weak-converse bounds in (2) and (8).

Appendix C: Asymptotic equipartition property for hypothesis testing relative entropy

In this appendix, we prove that the inequality in (38) holds whenever the states ρ and σ involved act on a separable Hilbert space. Here we take the convention, for convenience, that all logarithms are with respect to the natural base, but we note that the bound (C3) applies equally well for the binary logarithm just by rescaling.

The following proposition is available as [78, Eq. (6.5)] and restated as [61, Corollary 2]:

Proposition 1 ([78, Eq. (6.5)]) *Let ρ and σ be faithful states acting on a separable Hilbert space $\mathcal{H}$, let Λ be a measurement operator acting on $\mathcal{H}$ and such that $0 \leq \Lambda \leq I$, and let $v, \theta \in \mathbb{R}$. Then*

$$e^{-\theta} \operatorname{Tr}\{(I-\Lambda)\rho\} + \operatorname{Tr}\{\Lambda\sigma\} \geq \frac{e^{-\theta}}{1+e^{v-\theta}} \Pr\{X \leq v\}, \tag{C1}$$

where X is a random variable taking values $\log(\lambda_x/\mu_y)$ with probability $|\langle\psi_y|\phi_x\rangle|^2 \lambda_x$, where these quantities are defined in (31) and (32).

The following proposition is based on ideas given in [61]:

Proposition 2 *Let ρ and σ be faithful states acting on a separable Hilbert space $\mathcal{H}$, such that*

$$D(\rho\|\sigma),\ V(\rho\|\sigma),\ T(\rho\|\sigma) < \infty, \quad V(\rho\|\sigma) > 0. \tag{C2}$$

Then the following bound holds for all $\varepsilon \in (0,1)$ and sufficiently large n:

$$D_H^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) \leq nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\Phi^{-1}(\varepsilon) + O(\log n). \tag{C3}$$

Proof. We follow the justification for Theorem 3 given in [61] closely, but we do make some slight changes after the first few steps. Let Λ^n be any measurement operator satisfying $\operatorname{Tr}\{(I^{\otimes n} - \Lambda^n)\,\rho^{\otimes n}\} \leq \varepsilon$. By applying the above proposition (making the replacements $\rho \to \rho^{\otimes n}$ and $\sigma \to \sigma^{\otimes n}$, so that X_n is a sum of n i.i.d. random variables, each having mean $D(\rho\|\sigma)$, variance $V(\rho\|\sigma)$, and third absolute central moment $T(\rho\|\sigma)$), we find that

$$\begin{aligned}
&\operatorname{Tr}\{\Lambda^n\sigma^{\otimes n}\} \\
&\geq e^{-\theta_n}\left(\frac{\Pr\{X_n \leq v_n\}}{1+e^{v_n-\theta_n}} - \operatorname{Tr}\{(I-\Lambda^n)\rho^{\otimes n}\}\right) &\text{(C4)}\\
&\geq e^{-\theta_n}\left(\frac{\Pr\{X_n \leq v_n\}}{1+e^{v_n-\theta_n}} - \varepsilon\right). &\text{(C5)}
\end{aligned}$$

The Berry–Esseen theorem [27, 28] implies for any real number a that

$$\Pr\left\{\frac{X_n - nD(\rho\|\sigma)}{\sqrt{nV(\rho\|\sigma)}} \leq a\right\} \geq \Phi(a) - K_{\rho,\sigma}\, n^{-1/2}, \tag{C6}$$

where

$$K_{\rho,\sigma} \equiv \frac{C\,T(\rho\|\sigma)}{[V(\rho\|\sigma)]^{3/2}} \tag{C7}$$

and $C \in (0, 0.4748)$ [27, 28]. It is clear that $K_{\rho,\sigma}$ is a strictly positive constant $> C$ due to the assumption in (C2) and the fact that $T(\rho\|\sigma) \geq [V(\rho\|\sigma)]^{3/2}$ [28]. Let us set

$$v_n = nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\Phi^{-1}(\varepsilon + (2+K_{\rho,\sigma})n^{-1/2}), \tag{C8}$$

and note that we require sufficiently large n here, so that the argument to Φ^{-1} is $\in (0,1)$. We then find that

$$\operatorname{Tr}\{\Lambda^n\sigma^{\otimes n}\} \geq e^{-\theta_n}\left(\frac{\varepsilon + 2n^{-1/2}}{1+e^{v_n-\theta_n}} - \varepsilon\right). \tag{C9}$$

Now choosing $\theta_n = v_n + \frac{1}{2}\log n$, we get that

$$\begin{aligned}
&\operatorname{Tr}\{\Lambda^n\sigma^{\otimes n}\} \geq \\
&\left[e^{-nD(\rho\|\sigma) - \sqrt{nV(\rho\|\sigma)}\Phi^{-1}(\varepsilon + (2+K_{\rho,\sigma})n^{-1/2}) - \frac{1}{2}\log n}\right] \times \\
&\qquad\left(\frac{1}{1+n^{-1/2}}\right), &\text{(C10)}
\end{aligned}$$

so that the following inequality holds for sufficiently large n:

$$\begin{aligned}
&-\log\operatorname{Tr}\{\Lambda^n\sigma^{\otimes n}\} \leq \\
&\quad nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\Phi^{-1}(\varepsilon) + O(\log n). &\text{(C11)}
\end{aligned}$$

In the last line, we have invoked [58, Footnote 6], which in turn is an invocation of Taylor's theorem: for f continuously differentiable, c a positive constant, and $n \geq n_0$, the following equality holds

$$\sqrt{n}f(x + c/\sqrt{n}) = \sqrt{n}f(x) + cf'(a) \tag{C12}$$

for some $a \in [x, x + c/\sqrt{n_0}]$. ∎

Appendix D: Finiteness of the third absolute central moment of the log likelihood ratio for quantum Gaussian states

We argue in this final appendix that $T(\rho\|\sigma)$, the third absolute central moment of the log-likelihood ratio of two finite-energy, zero-mean Gaussian states ρ and σ, is finite. By definition, we have that

$$T(\rho\|\sigma) = \sum_{x,y} |\langle\psi_y|\phi_x\rangle|^2 \lambda_x \left|\log_2(\lambda_x/\mu_y) - D(\rho\|\sigma)\right|^3, \tag{D1}$$

where the spectral decompositions of ρ and σ are given by

$$\rho = \sum_x \lambda_x |\phi_x\rangle\langle\phi_x|, \qquad \sigma = \sum_y \mu_y |\psi_y\rangle\langle\psi_y|. \tag{D2}$$

By concavity of $x^{3/4}$ for $x \geq 0$, it follows that

$$\begin{aligned}
&T(\rho\|\sigma) \\
&= \sum_{x,y} |\langle\psi_y|\phi_x\rangle|^2 \lambda_x \left[\left|\log_2(\lambda_x/\mu_y) - D(\rho\|\sigma)\right|^4\right]^{3/4} \\
&\leq \left[\sum_{x,y} |\langle\psi_y|\phi_x\rangle|^2 \lambda_x \left|\log_2(\lambda_x/\mu_y) - D(\rho\|\sigma)\right|^4\right]^{3/4} \\
&= \left[\sum_{x,y} |\langle\psi_y|\phi_x\rangle|^2 \lambda_x \left(\log_2(\lambda_x/\mu_y) - D(\rho\|\sigma)\right)^4\right]^{3/4}, &\text{(D3)}
\end{aligned}$$

and so we aim to show that this latter quantity is finite. For zero-mean, m-mode faithful Gaussian states, the Williamson theorem [40] implies that their spectral decompositions are as follows:

$$\rho = U_\rho \left(\bigotimes_{i=1}^{m} \theta(N_\rho^i) \right) U_\rho^\dagger, \tag{D4}$$

$$\sigma = U_\sigma \left(\bigotimes_{i=1}^{m} \theta(N_\sigma^i) \right) U_\sigma^\dagger, \tag{D5}$$

where U_ρ and U_σ denote Gaussian unitaries that can be generated by a Hamiltonian no more than quadratic in the position- and momentum-quadrature operators, $N_\rho^i, N_\sigma^i > 0$ for all i, and $\theta(N)$ denotes a thermal state of mean photon number N:

$$\theta(N) = \frac{1}{N+1} \sum_{n=0}^{\infty} \left(\frac{N}{N+1} \right)^n |n\rangle\langle n|, \tag{D6}$$

with $|n\rangle$ denoting a photonic number state. Introducing the multi-index notation $|\vec{n}\rangle = |n_1\rangle \cdots |n_m\rangle$, we can then write the overlap $|\langle \psi_y | \phi_x \rangle|^2$ as $\left| \langle \vec{l} | U_\sigma^\dagger U_\rho | \vec{n} \rangle \right|^2$. This conditional probability distribution represents the probability of detecting the photon numbers $\vec{l}$ if the photon number state $|\vec{n}\rangle$ is prepared and transmitted through the Gaussian unitary $U_\sigma^\dagger U_\rho \equiv V$. This distribution has well defined (finite) higher moments with respect to photon number. Setting $\hat{n}_i$ to be the photon number operator for the ith mode, this claim follows because the kth moment of the conditional probability distribution $\left| \langle \vec{l} | U_\sigma^\dagger U_\rho | \vec{n} \rangle \right|^2$ is given by

$$\begin{aligned} &\mathrm{Tr}\left\{ V|\vec{n}\rangle\langle\vec{n}|V^\dagger \left(\sum_{i=1}^{m} \hat{n}_i \right)^k \right\} \\ &\qquad = \mathrm{Tr}\left\{ |\vec{n}\rangle\langle\vec{n}| \left(\sum_{i=1}^{m} V^\dagger \hat{n}_i V \right)^k \right\}. \end{aligned} \tag{D7}$$

Since V is a Gaussian unitary generated by a Hamiltonian no more than quadratic in the position and momentum-quadrature operators [34], each $V^\dagger \hat{n}_i V$ is a bounded linear combination of position and momentum-quadrature operators and so $\left(\sum_{i=1}^{m} V^\dagger \hat{n}_i V \right)^k$ is as well since k is finite. Given that the photon number states have bounded moments, we can conclude that (D7) is finite. The eigenvalues λ_x and μ_y in this case are given by

$$\prod_{i=1}^{m} \left[\frac{1}{N_\rho^i + 1} \left(\frac{N_\rho^i}{N_\rho^i + 1} \right)^{n_i} \right], \tag{D8}$$

$$\prod_{i=1}^{m} \left[\frac{1}{N_\sigma^i + 1} \left(\frac{N_\sigma^i}{N_\sigma^i + 1} \right)^{l_i} \right], \tag{D9}$$

and indexed by the multi-indices $\vec{n}$ and $\vec{l}$, respectively. The distribution in (D8) has well defined (finite) higher moments with respect to photon number because it is a product of geometric distributions. We can then write $\log_2(\lambda_x/\mu_y) = \log_2(\lambda_x) - \log_2(\mu_y)$ as

$$\begin{aligned} \sum_{i=1}^{m} \log_2\left(\frac{N_\sigma^i + 1}{N_\rho^i + 1} \right) + n_i \log_2\left(\frac{N_\rho^i}{N_\rho^i + 1} \right) \\ - l_i \log_2\left(\frac{N_\sigma^i}{N_\sigma^i + 1} \right). \end{aligned} \tag{D10}$$

Thus, after expanding, the last quantity in brackets in (D3) is equal to an expression involving no more than the fourth moments of photon numbers, but we have already argued that this is finite for the distributions under question. As a consequence, we can conclude that $T(\rho\|\sigma)$ is finite whenever ρ and σ are zero-mean, finite-energy, faithful Gaussian states.

[1] Alexander S. Holevo. *Quantum systems, channels, information: a mathematical introduction*, volume 16. Walter de Gruyter, 2012.

[2] Masahito Hayashi. *Quantum Information: An Introduction*. Springer, 2006.

[3] Mark M. Wilde. *From Classical to Quantum Shannon Theory*. March 2016. arXiv:1106.1445v7.

[4] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, pages 175–179, Bangalore, India, December 1984.

[5] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, August 1991.

[6] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. The squashed entanglement of a quantum channel. *IEEE Transactions on Information Theory*, 60(8):4987–4998, August 2014. arXiv:1310.0129.

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

[8] Kaushik P. Seshadreesan, Masahiro Takeoka, and Mark M. Wilde. Bounds on entanglement distillation and

secret key agreement for quantum broadcast channels. *IEEE Transactions on Information Theory*, 62(5):2849–2866, May 2016. arXiv:1503.08139.

[9] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. April 2016. arXiv:1510.08863v5.

[10] Kenneth Goodenough, David Elkouss, and Stephanie Wehner. Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels. *New Journal of Physics*, 18(6):063005, June 2016. arXiv:1511.08710.

[11] Masahiro Takeoka, Kaushik P. Seshadreesan, and Mark M. Wilde. Unconstrained distillation capacities of a pure-loss bosonic broadcast channel. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 2484–2488, July 2016.

[12] Koji Azuma, Akihiro Mizutani, and Hoi-Kwong Lo. Fundamental rate-loss trade-off for the quantum internet. *Nature Communications*, 7:13523, November 2016. arXiv:1601.02933.

[13] Mark M. Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. *IEEE Transactions on Information Theory*, 63(3):1792–1817, March 2017. arXiv:1602.08898.

[14] Matthias Christandl and Alexander Müller-Hermes. Relative entropy bounds on quantum, private and repeater capacities. *Communications in Mathematical Physics*, 353(2):821–852, July 2017. arXiv:1604.03448.

[15] Mark M. Wilde. Squashed entanglement and approximate private states. *Quantum Information Processing*, 15(11):4563–4580, November 2016. arXiv:1606.08028.

[16] Stefan Bäuml and Koji Azuma. Fundamental limitation on quantum broadcast networks. *Quantum Science and Technology*, 2(2):024004, June 2017. arXiv:1609.03994.

[17] Filip Rozpedek, Kenneth Goodenough, Jeremy Ribeiro, Norbert Kalb, Valentina Caprara Vivoli, Andreas Reiserer, Ronald Hanson, Stephanie Wehner, and David Elkouss. Realistic parameter regimes for a single sequential quantum repeater. May 2017. arXiv:1705.00043.

[18] Masahiro Takeoka, Kaushik P. Seshadreesan, and Mark M. Wilde. Unconstrained capacities of quantum key distribution and entanglement distillation for pure-loss bosonic broadcast channels. June 2017. arXiv:1706.06746.

[19] Norbert Lütkenhaus and Saikat Guha. Quantum repeaters: Objectives, definitions and architectures. Available at `http://wqrn.pratt.duke.edu/presentations.html`, May 2015.

[20] Ligong Wang and Renato Renner. One-shot classical-quantum capacity and hypothesis testing. *Physical Review Letters*, 108(20):200501, May 2012. arXiv:1007.5456.

[21] William Matthews and Stephanie Wehner. Finite blocklength converse bounds for quantum channels. *IEEE Transactions on Information Theory*, 60(11):7317–7329, November 2014. arXiv:1210.4722.

[22] Horace Yuen and Jeffrey H. Shapiro. Optical communication with two-photon coherent states–Part I: Quantum-state propagation and quantum-noise. *IEEE Transactions on Information Theory*, 24(6):657–668, November 1978.

[23] Jeffrey H. Shapiro. The quantum theory of optical communications. *IEEE Journal of Selected Topics in Quantum Electronics*, 15(6):1547–1569, November 2009.

[24] Ryo Namiki and Takuya Hirano. Practical limitation for continuous-variable quantum cryptography using coherent states. *Physical Review Letters*, 92(11):117901, March 2004. arXiv:quant-ph/0403115.

[25] Jérôme Lodewyck, Thierry Debuisschert, Rosa Tualle-Brouri, and Philippe Grangier. Controlling excess noise in fiber-optics continuous-variable quantum key distribution. *Physical Review A*, 72(5):050303, November 2005. arXiv:quant-ph/0511104.

[26] Pietro Liuzzo-Scorpo, Andrea Mari, Vittorio Giovannetti, and Gerardo Adesso. Optimal continuous variable quantum teleportation with limited resources. *Physical Review Letters*, 119(12):120503, September 2017. arXiv:1705.03017.

[27] V. Yu. Korolev and Irina G. Shevtsova. On the upper bound for the absolute constant in the Berry-Esseen inequality. *Theory of Probability & Its Applications*, 54(4):638–658, November 2010.

[28] Irina Shevtsova. On the absolute constants in the Berry-Esseen type inequalities for identically distributed summands. November 2011. arXiv:1111.6554.

[29] Yury Polyanskiy, H. Vincent Poor, and Sergio Verdú. Channel coding rate in the finite blocklength regime. *IEEE Transactions on Information Theory*, 56(5):2307–2359, May 2010.

[30] Yury Polyanskiy. *Channel coding: non-asymptotic fundamental limits*. PhD thesis, Princeton University, November 2010.

[31] Yury Polyanskiy. Finite blocklength methods in channel coding. Tutorial at the 2013 International Symposium on Information Theory, 2013. Available at `http://people.lids.mit.edu/yp/homepage/data/ISIT13_tutorial.pdf`.

[32] Marco Tomamichel, Mario Berta, and Joseph M. Renes. Quantum coding with finite resources. *Nature Communications*, 7:11419, May 2016. arXiv:1504.04617.

[33] Gerardo Adesso, Sammy Ragy, and Antony R. Lee. Continuous variable quantum information: Gaussian states and beyond. *Open Systems and Information Dynamics*, 21(01–02):1440001, June 2014. arXiv:1401.4679.

[34] Alessio Serafini. *Quantum Continuous Variables*. CRC Press, 2017.

[35] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, November 1996. arXiv:quant-ph/9604024.

[36] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Physical Review A*, 60(3):1888–1898, September 1999. arXiv:quant-ph/9807091.

[37] Michael M. Wolf, David Pérez-García, and Geza Giedke. Quantum capacities of bosonic channels. *Physical Review Letters*, 98(13):130501, March 2007. arXiv:quant-ph/0606132.

[38] Julien Niset, Jaromír Fiurasek, and Nicolas J. Cerf. No-go theorem for Gaussian quantum error correction. *Physical Review Letters*, 102(12):120501, March 2009. arXiv:0811.3128.

[39] Alexander Müller-Hermes. Transposition in quantum information theory. Master's thesis, Technical University of Munich, September 2012.

[40] John Williamson. On the algebraic problem concerning the normal forms of linear dynamical systems. *American Journal of Mathematics*, 58(1):141–163, January 1936.

[41] Xiao-yu Chen. Gaussian relative entropy of entanglement. *Physical Review A*, 71(6):062320, June 2005. arXiv:quant-ph/0402109.

[42] Ole Krueger. *Quantum Information Theory with Gaussian Systems*. PhD thesis, Technische Universität Braunschweig, April 2006. Available at `https://publikationsserver.tu-braunschweig.de/receive/dbbs_mods_00020741`.

[43] Alexander S. Holevo. The entropy gain of infinite-dimensional quantum channels. *Doklady Mathematics*, 82(2):730–731, October 2010. arXiv:1003.5765.

[44] Lu-Ming Duan, G. Giedke, J. I. Cirac, and P. Zoller. Inseparability criterion for continuous variable systems. *Physical Review Letters*, 84(12):2722–2725, March 2000. arXiv:quant-ph/9908056.

[45] R. Simon. Peres-Horodecki separability criterion for continuous variable systems. *Physical Review Letters*, 84(12):2726–2729, March 2000. arXiv:quant-ph/9909044.

[46] Alessio Serafini, Fabrizio Illuminati, and Silvio De Siena. Symplectic invariants, entropic measures and correlations of gaussian states. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 37(2):L21, January 2004. arXiv:quant-ph/0307073.

[47] Gerardo Adesso and Fabrizio Illuminati. Gaussian measures of entanglement versus negativities: Ordering of two-mode Gaussian states. *Physical Review A*, 72(3):032334, September 2005. arXiv:quant-ph/0506124.

[48] Filippo Caruso, Jens Eisert, Vittorio Giovannetti, and Alexander S. Holevo. Multi-mode bosonic Gaussian channels. *New Journal of Physics*, 10:083030, August 2008. arXiv:0804.0511.

[49] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, March 1993.

[50] Samuel L. Braunstein and H. J. Kimble. Teleportation of continuous quantum variables. *Physical Review Letters*, 80(4):869–872, January 1998.

[51] Reinhard F. Werner. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, 34(35):7081, September 2001. arXiv:quant-ph/0003070.

[52] Mark M. Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. January 2016. 1602.08898v1.

[53] Ryo Namiki. Teleportation stretching for lossy Gaussian channels. March 2016. arXiv:1603.05292.

[54] Ryszard Horodecki, Pawel Horodecki, Michal Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, June 2009. arXiv:quant-ph/0702225.

[55] Hisaharu Umegaki. Conditional expectations in an operator algebra IV (entropy and information). *Kodai Mathematical Seminar Reports*, 14(2):59–85, 1962.

[56] Göran Lindblad. Entropy, information and quantum measurements. *Communications in Mathematical Physics*, 33(4):305–322, December 1973.

[57] Ke Li. Second order asymptotics for quantum hypothesis testing. *Annals of Statistics*, 42(1):171–189, February 2014. arXiv:1208.1400.

[58] Marco Tomamichel and Masahito Hayashi. A hierarchy of information quantities for finite block length analysis of quantum tasks. *IEEE Transactions on Information Theory*, 59(11):7693–7710, November 2013. arXiv:1208.1478.

[59] Francesco Buscemi and Nilanjana Datta. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Transactions on Information Theory*, 56(3):1447–1460, March 2010. arXiv:0902.0158.

[60] Mark M. Wilde, Marco Tomamichel, Seth Lloyd, and Mario Berta. Gaussian hypothesis testing and quantum illumination. *Physical Review Letters*, 119(12):120501, September 2017. arXiv:1608.06991.

[61] Nilanjana Datta, Yan Pautrat, and Cambyse Rouzé. Second-order asymptotics for quantum hypothesis testing in settings beyond i.i.d. - quantum lattice systems and more. *Journal of Mathematical Physics*, 57(6):062207, June 2016. arXiv:1510.04682.

[62] Vlatko Vedral and Martin B. Plenio. Entanglement measures and purification procedures. *Physical Review A*, 57(3):1619–1633, March 1998. arXiv:quant-ph/9707035.

[63] Reinhard F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277–4281, October 1989.

[64] Fernando G. S. L. Brandao and Nilanjana Datta. One-shot rates for entanglement manipulation under non-entangling maps. *IEEE Transactions on Information Theory*, 57(3):1754–1760, March 2011. arXiv:0905.2673.

[65] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94(16):160502, April 2005. arXiv:quant-ph/0309110.

[66] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, April 2009. arXiv:quant-ph/0506189.

[67] Mathematica files are available in the source files of our arXiv post.

[68] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3:634, January 2012. arXiv:1103.4130.

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

[70] Kamil Brádler, Patrick Hayden, and Prakash Panangaden. Quantum communication in Rindler spacetime. *Communications in Mathematical Physics*, 312(2):361–398, June 2012. arXiv:1007.0997.

[71] Kamil Brádler and Christoph Adami. Black holes as bosonic Gaussian channels. *Physical Review D*, 92(2):025030, July 2015. arXiv:1405.1097.

[72] Haoyu Qi and Mark M. Wilde. Capacities of quantum amplifier channels. *Physical Review A*, 95(1):012339, January 2017. arXiv:1605.04922.

[73] R. Laurenza, S. L. Braunstein, and S. Pirandola. arXiv:1706.06065.

[74] Benjamin Schumacher and Michael A. Nielsen. Quantum data processing and error correction. *Physical Review A*, 54(4):2629–2635, October 1996. arXiv:quant-ph/9604022.

[75] Igor Devetak, Marius Junge, Christopher King, and Mary Beth Ruskai. Multiplicativity of completely bounded p-norms implies a new additivity result. *Communications in Mathematical Physics*, 266(1):37–63, August 2006. arXiv:quant-ph/0506196.

[76] Mark M. Wilde, Joseph M. Renes, and Saikat Guha. Second-order coding rates for pure-loss bosonic channels. *Quantum Information Processing*, 15(3):1289–1308, March 2016. arXiv:1408.5328.

[77] Göran Lindblad. Completely positive maps and entropy inequalities. *Communications in Mathematical Physics*, 40(2):147–151, June 1975.

[78] V. Jaksic, Y. Ogata, C.-A. Pillet, and R. Seiringer. Quantum hypothesis testing and non-equilibrium statistical mechanics. *Reviews in Mathematical Physics*, 24(06):1230002, 2012. arXiv:1109.3804.