

The squashed entanglement of the noiseless quantum Gaussian attenuator and amplifier

Giacomo De Palma^{1, a)}

*QMATH, Department of Mathematical Sciences, University of Copenhagen,
Universitetsparken 5, 2100 Copenhagen, Denmark*

(Dated: 5 November 2019)

We determine the maximum squashed entanglement achievable between sender and receiver of the noiseless quantum Gaussian attenuators and amplifiers, and prove that it is achieved sending half of an infinitely squeezed two-mode vacuum state. The key ingredient of the proof is a lower bound to the squashed entanglement of the quantum Gaussian states obtained applying a two-mode squeezing operation to a quantum thermal Gaussian state tensored with the vacuum state. This is the first lower bound to the squashed entanglement of a quantum Gaussian state, and opens the way to determine the squashed entanglement of all quantum Gaussian channels. Moreover, we determine the classical squashed entanglement of the quantum Gaussian states above, and show that it is strictly larger than their squashed entanglement. This is the first time that the classical squashed entanglement of a mixed quantum Gaussian state is determined.

^{a)}Electronic mail: giacomo.depalma@math.ku.dk

I. INTRODUCTION

The squashed entanglement of a bipartite quantum state ρ_{AB} is the infimum over all its possible extensions ρ_{ABR} of half of the quantum mutual information between the quantum systems A and B conditioned on the quantum system R ¹⁻⁹:

$$E_{\text{sq}}(\rho_{AB}) = \frac{1}{2} \inf \{ I(A; B|R)_{\rho_{ABR}} : \text{Tr}_R \rho_{ABR} = \rho_{AB} \}. \quad (1)$$

Here the quantum conditional mutual information is defined as¹⁰

$$I(A; B|R) = S(A|R) + S(B|R) - S(AB|R), \quad (2)$$

where $S(X|Y)$ is the quantum conditional entropy¹⁰⁻¹².

The squashed entanglement is one of the two main entanglement measures in quantum communication theory: together with the relative entropy of entanglement^{13,14}, it provides the best known upper bound to the length of a shared secret key that can be generated by two parties holding many copies of the quantum state^{7,15-17}. Moreover, it has applications in recoverability theory^{18,19} and multiparty information theory²⁰⁻²².

Any entanglement measure for quantum states can be extended to quantum channels defining it as the maximum entanglement achievable between sender and receiver. The relative entropy of entanglement of several quantum channels has been determined in 23. The squashed entanglement of a quantum channel Φ ²⁴ is the maximum squashed entanglement achievable between sender and receiver:

$$E_{\text{sq}}(\Phi) = \sup_{\rho_{AB}} E_{\text{sq}}((\mathbb{I}_A \otimes \Phi)(\rho_{AB})), \quad (3)$$

where the sender generates the bipartite quantum state ρ_{AB} , keeps the quantum system A and sends the quantum system B to the receiver through Φ . In the same way as the squashed entanglement of a quantum state is an upper bound to the distillable key of the state, the squashed entanglement of a quantum channel is an upper bound to the capacity of the channel to generate a secret key shared between sender and receiver^{24,25}.

We prove a lower bound on the squashed entanglement of the quantum Gaussian states obtained applying a two-mode squeezing operation to a thermal quantum Gaussian state tensored with the vacuum state (Theorem 1; see (21) for the definition of the states). This is the first lower bound to the squashed entanglement of a quantum Gaussian state. Previous results restrict the optimization in (1) to Gaussian extensions and consider the 2-Rényi entropy instead of the von

Neumann entropy²⁶. Our bound is optimal in the limit of infinite energy and extremely tight already from one average photon (Figure 1). Lower bounds to the squashed entanglement are notoriously difficult to prove, since the optimization in (1) over all the possible extensions of the quantum state is almost never analytically treatable. We overcome this difficulty with the quantum conditional Entropy Power Inequality^{27–30}, which holds for any conditioning quantum system.

We apply Theorem 1 to prove our main result: a new lower bound to the squashed entanglement of the noiseless quantum Gaussian attenuators and amplifiers (Theorem 2). This lower bound matches the upper bound proven in 24, 31–33. Therefore, Theorem 2 determines the maximum squashed entanglement achievable between sender and receiver for the noiseless quantum Gaussian attenuators and amplifiers, and proves that it is achieved sending half of an infinitely squeezed two-mode vacuum state. The maximum achievable squashed entanglement is proved to be $\ln \frac{1+\eta}{1-\eta}$ for the attenuator with attenuation parameter $0 \leq \eta \leq 1$ and $\ln \frac{\kappa+1}{\kappa-1}$ for the amplifier with amplification parameter $\kappa \geq 1$. The noiseless quantum Gaussian attenuator and amplifier play a key role in quantum communication theory. The amplifier provides the mathematical model for the amplification of electromagnetic signals, and the attenuator provides the mathematical model for the propagation of electromagnetic signals through optical fibers^{34–38}, which are the main platform for quantum key distribution and for the transmission of quantum states in the forthcoming quantum internet^{37,39–55}. A proof based on the relative entropy of entanglement and on the teleportation stretching technique has determined the capacity of the noiseless quantum Gaussian attenuator and amplifier to generate a shared secret to be $\ln \frac{1}{1-\eta}$ and $\ln \frac{\kappa}{\kappa-1}$ nats per channel use, respectively^{23,56} (later a generalization to repeaters^{47,54} was proved, and strong converse bounds^{57–59} were also considered). Theorem 2 proves that these channels can generate a squashed entanglement between sender and receiver strictly larger than their secret key capacity.

A fundamental question about the squashed entanglement of a quantum state is whether the minimization in (1) can be restricted to classical extensions⁶. The answer is known to be negative in general⁶⁰, and this has led to the definition to the classical squashed entanglement^{16,22,61–64}, which has later found an operational interpretation as the minimum cost of classical communication required for assisted entanglement dilution⁶⁵. We determine the classical squashed entanglement of the quantum Gaussian states (21) and prove that it is achieved by a Gaussian extension and strictly larger than their squashed entanglement, with equality only when the state is pure or separable (Theorem 3, Figure 1). This is the first time that the classical squashed entanglement of a mixed quantum Gaussian state is determined. The proof is based on the one-mode version of

the constrained minimum output entropy conjecture for the noiseless quantum Gaussian amplifier and for its complementary channel^{66–83}. Theorem 3 also proves that the multi-mode version of the conjecture implies that the classical squashed entanglement of the quantum Gaussian states (21) does not decrease regularizing over many copies of the state. Therefore, assuming the multi-mode conjecture, the asymptotic classical squashed entanglement of the states (21) coincides with their classical squashed entanglement and is strictly larger than their squashed entanglement.

The paper is structured as follows. In section II we introduce quantum Gaussian systems, states and channels. In section III we prove the lower bound to the squashed entanglement of the quantum Gaussian states (21) (Theorem 1) and we determine the squashed entanglement of the noiseless quantum Gaussian attenuator and amplifier (Theorem 2). In section IV we determine the classical squashed entanglement of the quantum Gaussian state (21). Conclusions and open problems are presented in section V. In section A, we present the entropic inequalities employed in the proofs.

II. QUANTUM GAUSSIAN SYSTEMS

A one-mode quantum Gaussian system is the mathematical model for a harmonic oscillator or for a mode of the electromagnetic radiation. The Hilbert space of a one-mode quantum Gaussian system is the irreducible representation of the canonical commutation relation^{37,38}, [11, Chapter 12]

$$[Q, P] = \mathbb{I}, \quad (4)$$

where Q and P are the quadrature operators, which for the harmonic oscillator represent position and momentum. The Hamiltonian that counts the number of excitations or photons is

$$H = a^\dagger a, \quad (5)$$

where

$$a = \frac{Q + iP}{\sqrt{2}} \quad (6)$$

is the ladder operator. The vector annihilated by a is the vacuum and is denoted by $|0\rangle$. A quantum Gaussian state is a quantum state proportional to the exponential of a quadratic polynomial in Q and P . The most important quantum Gaussian states are the thermal Gaussian states, where the

polynomial is proportional to the Hamiltonian (5):

$$\omega(E) = \frac{1}{(E+1)} \left(\frac{E}{E+1} \right)^{a^\dagger a}, \quad (7)$$

and $E \geq 0$ is the average energy:

$$\text{Tr} \left[\omega(E) a^\dagger a \right] = E. \quad (8)$$

We notice that $\omega(0) = |0\rangle\langle 0|$ is the vacuum state. The von Neumann entropy of $\omega(E)$ is

$$S(\omega(E)) = (E+1) \ln(E+1) - E \ln E =: g(E). \quad (9)$$

An n -mode Gaussian quantum system is the union of n one-mode Gaussian quantum systems, and its Hilbert space is the n -th tensor power of the Hilbert space of a one-mode Gaussian quantum system. Let $R_1 = Q_1, R_2 = P_1, \dots, R_{2n-1} = Q_n, R_{2n} = P_n$ be the quadrature operators of the n modes, satisfying the canonical commutation relations

$$[R_i, R_j] = i\Delta_{ij}\mathbb{I}, \quad i, j = 1, \dots, 2n, \quad (10)$$

where

$$\Delta = \bigoplus_{k=1}^n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad (11)$$

is the symplectic form. The covariance matrix of a quantum state ρ is the $2n \times 2n$ positive real matrix given by

$$\sigma(\rho)_{ij} = \frac{1}{2} \text{Tr} \left[\rho \{R_i - \text{Tr}[\rho R_i], R_j - \text{Tr}[\rho R_j]\} \right], \quad i, j = 1, \dots, 2n, \quad (12)$$

where

$$\{X, Y\} = XY + YX \quad (13)$$

is the anti-commutator. The eigenvalues of the matrix $\Delta^{-1}\sigma$ are pure imaginary and pairwise opposite. Their absolute values are the symplectic eigenvalues of σ ¹¹. An n -mode quantum Gaussian state is a state proportional to the exponential of a quadratic polynomial in the quadratures. Its von Neumann entropy is⁸⁴

$$S = \sum_{k=1}^n g \left(\nu_k - \frac{1}{2} \right), \quad (14)$$

where ν_1, \dots, ν_n are the symplectic eigenvalues of its covariance matrix, and g is defined in (9).

Quantum Gaussian channels are the quantum channels that preserve the set of quantum Gaussian states. The most important families of quantum Gaussian channels are the beam-splitter,

the squeezing and the quantum Gaussian attenuators and amplifiers. The beam-splitter and the squeezing are the quantum counterparts of the classical linear mixing of random variables, and are the main transformations in quantum optics. Let A and B be one-mode quantum Gaussian systems with ladder operators a and b , respectively. The *beam-splitter* of transmissivity $0 \leq \eta \leq 1$ is implemented by the unitary operator

$$U_\eta = \exp\left(\left(a^\dagger b - b^\dagger a\right) \arccos \sqrt{\eta}\right), \quad (15)$$

and performs a linear rotation of the ladder operators [85, Section 1.4.2]:

$$\begin{aligned} U_\eta^\dagger a U_\eta &= \sqrt{\eta} a + \sqrt{1-\eta} b, \\ U_\eta^\dagger b U_\eta &= -\sqrt{1-\eta} a + \sqrt{\eta} b. \end{aligned} \quad (16)$$

The *squeezing*⁸⁶ of parameter $\kappa \geq 1$ is implemented by the unitary operator

$$U_\kappa = \exp\left(\left(a^\dagger b^\dagger - ab\right) \operatorname{arccosh} \sqrt{\kappa}\right), \quad (17)$$

and acts on the ladder operators as

$$\begin{aligned} U_\kappa^\dagger a U_\kappa &= \sqrt{\kappa} a + \sqrt{\kappa-1} b^\dagger, \\ U_\kappa^\dagger b U_\kappa &= \sqrt{\kappa-1} a^\dagger + \sqrt{\kappa} b. \end{aligned} \quad (18)$$

The noiseless quantum Gaussian attenuators model the attenuation affecting electromagnetic signals traveling through optical fibers or free space. The one-mode *noiseless quantum Gaussian attenuator* \mathcal{E}_η [36, case (C) with $k = \sqrt{\eta}$ and $N = 0$] can be implemented mixing the input state ρ with the one-mode vacuum state through a beam-splitter of transmissivity $0 \leq \eta \leq 1$:

$$\mathcal{E}_\eta(\rho) = \operatorname{Tr}_B \left[U_\eta (\rho \otimes |0\rangle\langle 0|) U_\eta^\dagger \right]. \quad (19)$$

The noiseless quantum Gaussian amplifiers model the amplification of electromagnetic signals. The one-mode *noiseless quantum Gaussian amplifier* \mathcal{A}_κ [36, case (C) with $k = \sqrt{\kappa}$ and $N = 0$] can be implemented performing a squeezing of parameter $\kappa \geq 1$ on the input state ρ and the one-mode vacuum state:

$$\mathcal{A}_\kappa(\rho) = \operatorname{Tr}_B \left[U_\kappa (\rho \otimes |0\rangle\langle 0|) U_\kappa^\dagger \right]. \quad (20)$$

III. SQUASHED ENTANGLEMENT

Let A and B be one-mode quantum Gaussian systems. For any $\kappa \geq 1$ and any $E \geq 0$ we consider the quantum Gaussian state

$$\rho_{AB}^{\kappa,E} = U_\kappa (\omega_A(E) \otimes |0\rangle_B \langle 0|) U_\kappa^\dagger, \quad (21)$$

where $\omega_A(E)$ is the thermal quantum Gaussian state on A with average energy E defined in (7), $|0\rangle_B$ is the vacuum state of B and U_κ is the two-mode squeezing operator on AB with squeezing parameter κ defined in (17).

Theorem 1. *For any $\kappa \geq 1$ and any $E \geq 0$, the squashed entanglement of the quantum Gaussian state $\rho_{AB}^{\kappa,E}$ defined in (21) satisfies*

$$\ln(2\kappa - 1) \leq E_{\text{sq}}(\rho_{AB}^{\kappa,E}) \leq g\left(\left(\kappa - \frac{1}{2}\right)E + \kappa - 1\right) - g\left(\frac{E}{2}\right). \quad (22)$$

Moreover, the gap between the upper and lower bound of (22) is at most $\ln \frac{e}{2} \simeq 0.31$, and tends to zero in the limit $E \rightarrow \infty$. We conjecture that the upper bound of (22) is the actual value of the squashed entanglement of $\rho_{AB}^{\kappa,E}$.

Proof. Let ρ_{ABR} be an extension of $\rho_{AB}^{\kappa,E}$. The quantum state $U_\kappa^\dagger \rho_{ABR} U_\kappa$ is an extension of $\omega_A(E) \otimes |0\rangle_B \langle 0|$, therefore it has the form $\omega_{AR} \otimes |0\rangle_B \langle 0|$ for some quantum state ω_{AR} that is an extension of $\omega_A(E)$. The quantum state ρ_{ABR} has then the form

$$\rho_{ABR} = U_\kappa (\omega_{AR} \otimes |0\rangle_B \langle 0|) U_\kappa^\dagger, \quad \text{Tr}_R \omega_{AR} = \omega_A(E). \quad (23)$$

Conversely, any state of the form (23) is an extension of $\rho_{AB}^{\kappa,E}$.

a. Lower bound The quantum conditional Entropy Power Inequality (Theorem 6) implies

$$\begin{aligned} I(A;B|R)_{\rho_{ABR}} &= S(A|R)_{\rho_{ABR}} + S(B|R)_{\rho_{ABR}} - S(AB|R)_{\rho_{ABR}} \\ &= S(A|R)_{\rho_{ABR}} + S(B|R)_{\rho_{ABR}} - S(A|R)_{\omega_{AR}} \\ &\geq \ln \left(2\kappa(\kappa - 1) \cosh S(A|R)_{\omega_{AR}} + \kappa^2 + (\kappa - 1)^2 \right) \\ &\geq 2 \ln(2\kappa - 1), \end{aligned} \quad (24)$$

where the last inequality is saturated when $S(A|R)_{\omega_{AR}} = 0$. The lower bound in (22) follows taking the infimum of the left-hand side of (24) over the extensions ρ_{ABR} .

b. Upper bound We consider the one-parameter family of extensions $\{\rho_{ABR}(\eta)\}_{0 \leq \eta \leq 1}$ of $\rho_{AB}^{\kappa, E}$ of the form (23) where R is a one-mode quantum Gaussian system and

$$\omega_{AR}(\eta) = (\mathbb{I}_A \otimes \mathcal{E}_\eta)(|\phi_E\rangle_{AR}\langle\phi_E|) \quad (25)$$

is the quantum Gaussian state obtained applying the noiseless quantum Gaussian attenuator with attenuation parameter η to half of the two-mode squeezed vacuum state $|\phi_E\rangle_{AR}$ with average energy per mode E . We leave η as a free parameter over which we will optimize in the end. The covariance matrix of $\omega_{AR}(\eta)$ is

$$\sigma(\omega_{AR}(\eta)) = \begin{pmatrix} (E + \frac{1}{2}) I_2 & \sqrt{\eta E (E + 1)} \sigma_Z \\ \sqrt{\eta E (E + 1)} \sigma_Z & (\eta E + \frac{1}{2}) I_2 \end{pmatrix}, \quad (26)$$

where

$$\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (27)$$

The symplectic eigenvalues of $\sigma(\omega_{AR}(\eta))$ are

$$v_+(\sigma(\omega_{AR}(\eta))) = (1 - \eta)E + \frac{1}{2}, \quad v_-(\sigma(\omega_{AR}(\eta))) = \frac{1}{2}, \quad (28)$$

hence

$$\begin{aligned} S(ABR)_{\rho_{ABR}(\eta)} &= S(AR)_{\omega_{AR}(\eta)} = g(v_+(\sigma(\omega_{AR}(\eta))) - \frac{1}{2}) + g(v_-(\sigma(\omega_{AR}(\eta))) - \frac{1}{2}) \\ &= g((1 - \eta)E), \\ S(R)_{\rho_{ABR}(\eta)} &= S(R)_{\omega_{AR}(\eta)} = g(\eta E). \end{aligned} \quad (29)$$

Let $\rho_{AR}(\eta)$ and $\rho_{BR}(\eta)$ be the marginals of $\rho_{ABR}(\eta)$ on AR and BR , respectively. They are the quantum Gaussian states with covariance matrices

$$\begin{aligned} \sigma(\rho_{AR}(\eta)) &= \begin{pmatrix} (\kappa(E + 1) - \frac{1}{2}) I_2 & \sqrt{\kappa \eta E (E + 1)} \sigma_Z \\ \sqrt{\kappa \eta E (E + 1)} \sigma_Z & (\eta E + \frac{1}{2}) I_2 \end{pmatrix}, \\ \sigma(\rho_{BR}(\eta)) &= \begin{pmatrix} ((\kappa - 1)(E + \frac{1}{2}) + \frac{\kappa}{2}) I_2 & \sqrt{(\kappa - 1) \eta E (E + 1)} I_2 \\ \sqrt{(\kappa - 1) \eta E (E + 1)} I_2 & (\eta E + \frac{1}{2}) I_2 \end{pmatrix}. \end{aligned} \quad (30)$$

Their symplectic eigenvalues are

$$\begin{aligned} v_+(\sigma(\rho_{AR}(\eta))) &= \kappa(E + 1) - \eta E - \frac{1}{2}, \\ v_+(\sigma(\rho_{BR}(\eta))) &= \kappa(E + 1) - (1 - \eta)E - \frac{1}{2}, \\ v_-(\sigma(\rho_{AR}(\eta))) &= v_-(\sigma(\rho_{BR}(\eta))) = \frac{1}{2}, \end{aligned} \quad (31)$$

hence

$$\begin{aligned} S(AR)_{\rho_{ABR}(\eta)} &= g(\kappa(E+1) - \eta E - 1), \\ S(BR)_{\rho_{ABR}(\eta)} &= g(\kappa(E+1) - (1-\eta)E - 1). \end{aligned} \quad (32)$$

Therefore, for any $0 \leq \eta \leq 1$ we have

$$\begin{aligned} E_{\text{sq}}(\rho_{AB}) &\leq \frac{1}{2} I(A; B|R)_{\rho_{ABR}(\eta)} \\ &= \frac{1}{2} (S(AR)_{\rho_{ABR}(\eta)} + S(BR)_{\rho_{ABR}(\eta)} - S(R)_{\rho_{ABR}(\eta)} - S(ABR)_{\rho_{ABR}(\eta)}) \\ &= \frac{1}{2} (\psi_{E,\kappa}(\eta) + \psi_{E,\kappa}(1-\eta)), \end{aligned} \quad (33)$$

where

$$\psi_{E,\kappa}(\eta) = g(\kappa E + \kappa - \eta E - 1) - g((1-\eta)E). \quad (34)$$

From Lemma 1 of section B, $\psi_{E,\kappa}$ is convex, hence from Jensen's inequality the minimum over $0 \leq \eta \leq 1$ of the right-hand side of (33) is achieved by $\eta = \frac{1}{2}$. Therefore,

$$E_{\text{sq}}(\rho_{AB}) \leq \psi_{E,\kappa}\left(\frac{1}{2}\right), \quad (35)$$

and the claim follows. We notice that $S(A|R)_{\omega_{AR}(\frac{1}{2})} = 0$, which is the same condition that saturates the last inequality of (24).

c. Gap Let

$$f(\kappa, E) = g\left(\left(\kappa - \frac{1}{2}\right)E + \kappa - 1\right) - g\left(\frac{E}{2}\right) - \ln(2\kappa - 1) \quad (36)$$

be the difference between the upper and lower bound of (22). Since $E \mapsto f(\kappa, E)$ is decreasing,

$$f(\kappa, E) \leq f(\kappa, 0) = g(\kappa - 1) - \ln(2\kappa - 1). \quad (37)$$

We have

$$\frac{\partial f}{\partial \kappa}(\kappa, 0) = \ln \frac{\kappa}{\kappa - 1} - \frac{2}{2\kappa - 1} \geq 0, \quad (38)$$

hence $\kappa \mapsto f(\kappa, 0)$ is increasing and

$$f(\kappa, 0) \leq \lim_{\kappa \rightarrow \infty} f(\kappa, 0) = \ln \frac{e}{2}. \quad (39)$$

□

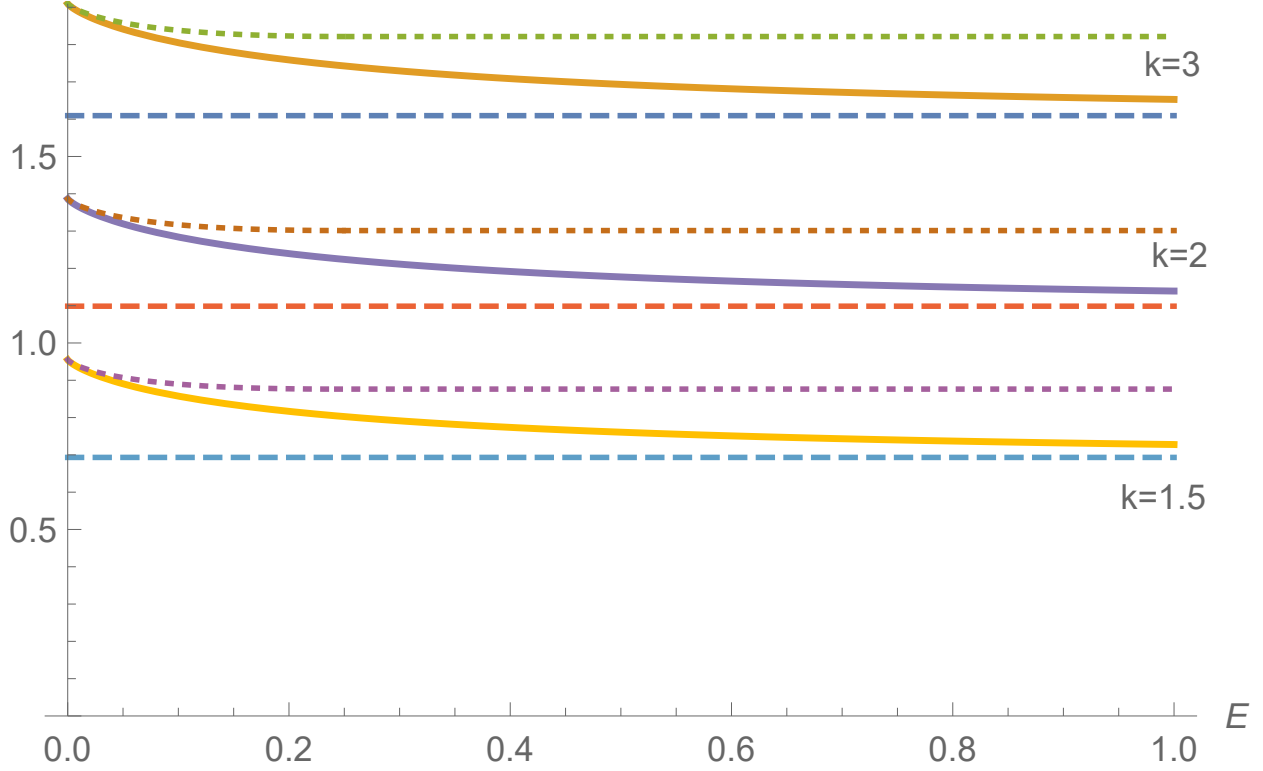


FIG. 1. Thick and dashed: the upper and lower bounds of Theorem 1 to the squashed entanglement of the quantum Gaussian state $\rho_{AB}^{\kappa, E}$ of (21) for $\kappa = 1.5, 2, 3$ and $0 \leq E \leq 1$. The bounds coincide in the limit of infinite average energy, but they are extremely close already from $E \simeq 1$. Dotted: the classical squashed entanglement of $\rho_{AB}^{\kappa, E}$ determined in Theorem 3 for the same values of κ and E .

Figure 1 shows the difference between the upper and lower bounds of (22), which is extremely small already from $E \simeq 1$.

Corollary 1 below provides the link between Theorem 1 and the noiseless quantum Gaussian attenuators and amplifiers. For any $E \geq 0$, let $|\phi_E\rangle_{AB}$ be the two-mode squeezed vacuum state on AB with average energy per mode E , which coincides with the quantum Gaussian state $\rho_{AB}^{\kappa', E'}$ of (21) with $\kappa' = E + 1$ and $E' = 0$.

Let $\gamma_{AB}^{\eta, E}$ be the quantum Gaussian state obtained sending the B system of $|\phi_E\rangle_{AB}$ through a noiseless quantum Gaussian attenuator with attenuation parameter $0 \leq \eta \leq 1$, and let $\gamma_{AB}^{\kappa, E}$ be the quantum Gaussian state obtained sending the A system of $|\phi_E\rangle_{AB}$ through a noiseless quantum Gaussian amplifier with amplification parameter $\kappa \geq 1$:

$$\gamma_{AB}^{\eta, E} = (\mathbb{I}_A \otimes \mathcal{E}_\eta)(|\phi_E\rangle_{AB}\langle\phi_E|), \quad \gamma_{AB}^{\kappa, E} = (\mathcal{A}_\kappa \otimes \mathbb{I}_B)(|\phi_E\rangle_{AB}\langle\phi_E|). \quad (40)$$

Corollary 1. *The squashed entanglement of the quantum Gaussian states $\gamma_{AB}^{\eta,E}$ and $\gamma_{AB}^{\kappa,E}$ defined in (40) satisfies*

$$\begin{aligned} \ln \frac{(1+\eta)E+1}{(1-\eta)E+1} &\leq E_{\text{sq}}\left(\gamma_{AB}^{\eta,E}\right) \leq g\left(\frac{1+\eta}{2}E\right) - g\left(\frac{1-\eta}{2}E\right), \\ \ln \frac{(\kappa+1)E+\kappa}{(\kappa-1)E+\kappa} &\leq E_{\text{sq}}\left(\gamma_{AB}^{\kappa,E}\right) \leq g\left(\frac{(\kappa+1)E+\kappa-1}{2}\right) - g\left(\frac{\kappa-1}{2}(E+1)\right). \end{aligned} \quad (41)$$

Moreover, the gap between the upper bounds and the respective lower bounds in (41) is at most $\ln \frac{e}{2} \simeq 0.31$. We conjecture that the actual value of the squashed entanglement of $\gamma_{AB}^{\eta,E}$ and $\gamma_{AB}^{\kappa,E}$ coincides with the upper bounds in (41).

Proof. We will prove that both the lower and the upper bounds of (41) follow from Theorem 1. While the lower bounds appear in this paper for the first time, the upper bounds have been proved also in 24, 31–33.

Let $\rho_{AB}^{\kappa',E'}$ be as in (21) with $\kappa' \geq 1$ and $E' \geq 0$. The covariance matrices of $\rho_{AB}^{\kappa',E'}$, $\gamma_{AB}^{\eta,E}$ and $\gamma_{AB}^{\kappa,E}$ are

$$\begin{aligned} \sigma\left(\rho_{AB}^{\kappa',E'}\right) &= \begin{pmatrix} (\kappa'(E'+1) - \frac{1}{2})I_2 & (E'+1)\sqrt{\kappa'(\kappa'-1)}\sigma_Z \\ (E'+1)\sqrt{\kappa'(\kappa'-1)}\sigma_Z & ((\kappa'-1)(E'+1) + \frac{1}{2})I_2 \end{pmatrix}, \\ \sigma\left(\gamma_{AB}^{\eta,E}\right) &= \begin{pmatrix} (E+\frac{1}{2})I_2 & \sqrt{\eta E(E+1)}\sigma_Z \\ \sqrt{\eta E(E+1)}\sigma_Z & (\eta E + \frac{1}{2})I_2 \end{pmatrix}, \\ \sigma\left(\gamma_{AB}^{\kappa,E}\right) &= \begin{pmatrix} (\kappa E + \kappa - \frac{1}{2})I_2 & \sqrt{\kappa E(E+1)}\sigma_Z \\ \sqrt{\kappa E(E+1)}\sigma_Z & (E + \frac{1}{2})I_2 \end{pmatrix}. \end{aligned} \quad (42)$$

For

$$\kappa' = \frac{E+1}{(1-\eta)E+1}, \quad E' = (1-\eta)E \quad (43)$$

we have $\sigma\left(\rho_{AB}^{\kappa',E'}\right) = \sigma\left(\gamma_{AB}^{\eta,E}\right)$, and therefore $\rho_{AB}^{\kappa',E'} = \gamma_{AB}^{\eta,E}$. Analogously, for

$$\kappa' = \frac{\kappa(E+1)}{(\kappa-1)E+\kappa}, \quad E' = (\kappa-1)(E+1) \quad (44)$$

we have $\sigma\left(\rho_{AB}^{\kappa',E'}\right) = \sigma\left(\gamma_{AB}^{\kappa,E}\right)$, and therefore $\rho_{AB}^{\kappa',E'} = \gamma_{AB}^{\kappa,E}$. The claim then follows from Theorem 1. \square

Remark 1. Since the squashed entanglement of any bipartite quantum state is lower than the squashed entanglement of the quantum Gaussian state with the same covariance matrix⁸⁷, the

upper bounds of (22) and (41) apply to any bipartite quantum state with covariance matrix as in (42).

We can now prove the main result of the paper.

Theorem 2. *The squashed entanglement of the noiseless quantum Gaussian attenuator with attenuation parameter $0 \leq \eta \leq 1$ and of the noiseless quantum Gaussian amplifier with amplification parameter $\kappa \geq 1$ is*

$$E_{\text{sq}}(\mathcal{E}_\eta) = \ln \frac{1+\eta}{1-\eta}, \quad E_{\text{sq}}(\mathcal{A}_\kappa) = \ln \frac{\kappa+1}{\kappa-1}, \quad (45)$$

and is asymptotically achieved sending half of a two-mode squeezed vacuum state $|\phi_E\rangle_{AB}$ in the limit $E \rightarrow \infty$ of infinite average energy or infinite squeezing.

Proof. The upper bounds

$$E_{\text{sq}}(\mathcal{E}_\eta) \leq \ln \frac{1+\eta}{1-\eta}, \quad E_{\text{sq}}(\mathcal{A}_\kappa) \leq \ln \frac{\kappa+1}{\kappa-1} \quad (46)$$

have been proved in 24, 31–33.

Given $E \geq 0$, let $\gamma_{AB}^{\eta,E}$ and $\gamma_{AB}^{\kappa,E}$ be as in (40). We have from Corollary 1

$$\begin{aligned} E_{\text{sq}}(\mathcal{E}_\eta) &\geq E_{\text{sq}}\left(\gamma_{AB}^{\eta,E}\right) \geq \ln \frac{(1+\eta)E+1}{(1-\eta)E+1}, \\ E_{\text{sq}}(\mathcal{A}_\kappa) &\geq E_{\text{sq}}\left(\gamma_{AB}^{\kappa,E}\right) \geq \ln \frac{(\kappa+1)E+\kappa}{(\kappa-1)E+\kappa}. \end{aligned} \quad (47)$$

Taking the limit $E \rightarrow \infty$ we get

$$E_{\text{sq}}(\mathcal{E}_\eta) \geq \ln \frac{1+\eta}{1-\eta}, \quad E_{\text{sq}}(\mathcal{A}_\kappa) \geq \ln \frac{\kappa+1}{\kappa-1}, \quad (48)$$

and the claim follows. \square

IV. CLASSICAL SQUASHED ENTANGLEMENT

The classical squashed entanglement^{16,22,61,63,64} has the same definition as the squashed entanglement with the minimization in (1) restricted to the classical extensions of the quantum state. A classical extension ρ_{ABR} of the quantum state ρ_{AB} is given by a probability measure ρ_R on a measure space \mathcal{R} and a set $\{\rho_{AB|R=r}\}_{r \in \mathcal{R}}$ of the states of the quantum system AB conditioned on $R = r$, such that the function $r \mapsto \rho_{AB|R=r}$ is measurable and

$$\int_{\mathcal{R}} \rho_{AB|R=r} d\rho_R(r) = \rho_{AB}. \quad (49)$$

The classical squashed entanglement of the bipartite quantum state ρ_{AB} is half of the infimum over all the classical extension ρ_{ABR} of the mutual information between the quantum systems A and B conditioned on the classical system R :

$$E_{\text{sq,c}}(\rho_{AB}) = \frac{1}{2} \inf \left\{ I(A;B|R)_{\rho_{ABR}} : \int_{\mathcal{R}} \rho_{AB|R=r} d\rho_R(r) = \rho_{AB} \right\}, \quad (50)$$

where the conditional mutual information is defined as

$$I(A;B|R)_{\rho_{ABR}} = \int_{\mathcal{R}} I(A;B)_{\rho_{AB|R=r}} d\rho_R(r). \quad (51)$$

The classical squashed entanglement is always not lower than the squashed entanglement, and can be strictly larger⁶⁰. A fundamental property of the squashed entanglement is its additivity with respect to the tensor product⁷: for any two bipartite quantum states $\rho_{A_1B_1}$ and $\rho_{A_2B_2}$,

$$E_{\text{sq}}(\rho_{A_1B_1} \otimes \rho_{A_2B_2}) = E_{\text{sq}}(\rho_{A_1B_1}) + E_{\text{sq}}(\rho_{A_2B_2}). \quad (52)$$

The classical squashed entanglement is subadditive with respect to the tensor product:

$$E_{\text{sq,c}}(\rho_{A_1B_1} \otimes \rho_{A_2B_2}) \leq E_{\text{sq,c}}(\rho_{A_1B_1}) + E_{\text{sq,c}}(\rho_{A_2B_2}), \quad (53)$$

but it is not known whether it is additive. This has led to the definition of the asymptotic classical squashed entanglement as the regularization of the classical squashed entanglement over many copies of the quantum state^{16,22,61}:

$$E_{\text{sq,c}}^{\infty}(\rho_{AB}) = \lim_{n \rightarrow \infty} \frac{E_{\text{sq,c}}(\rho_{AB}^{\otimes n})}{n}. \quad (54)$$

Thanks to the additivity of the squashed entanglement, the asymptotic classical squashed entanglement is still an upper bound to the squashed entanglement.

Here we determine the classical squashed entanglement of the Gaussian quantum states defined in (21) and show that it is achieved by a Gaussian extension and strictly larger than their squashed entanglement (see Figure 1 for the comparison). The proof exploits the constrained minimum output entropy conjecture for the one-mode noiseless quantum Gaussian amplifier and its complementary channel. We also show that the multi-mode generalization of the conjecture determines the asymptotic classical squashed entanglement of the Gaussian quantum states (21) and implies that it is equal to the classical squashed entanglement of one copy of the state, and therefore still strictly larger than the squashed entanglement.

Theorem 3. *The classical squashed entanglement of the Gaussian quantum state (21) is achieved by a Gaussian extension and is equal to*

$$E_{\text{sq,c}}\left(\rho_{AB}^{\kappa,E}\right) = \frac{1}{2} \min_{x \in [0,E]} h_{\kappa}(x), \quad (55)$$

where for any $x \geq 0$,

$$h_{\kappa}(x) = g(\kappa x + \kappa - 1) + g((\kappa - 1)(x + 1)) - g(x). \quad (56)$$

For any $E > 0$ and any $\kappa > 1$, the classical squashed entanglement of $\rho_{AB}^{\kappa,E}$ is strictly larger than its squashed entanglement:

$$E_{\text{sq,c}}\left(\rho_{AB}^{\kappa,E}\right) > E_{\text{sq}}\left(\rho_{AB}^{\kappa,E}\right). \quad (57)$$

Moreover, assuming Conjecture 1, the asymptotic classical squashed entanglement of $\rho_{AB}^{\kappa,E}$ coincides with its classical squashed entanglement:

$$E_{\text{sq,c}}^{\infty}\left(\rho_{AB}^{\kappa,E}\right) = E_{\text{sq,c}}\left(\rho_{AB}^{\kappa,E}\right). \quad (58)$$

Remark 2. Since the function $s \mapsto h_{\kappa}(g^{-1}(s))$ is strictly convex [79, Lemma 15] and

$$\left. \frac{d}{ds} h_{\kappa}(g^{-1}(s)) \right|_{s=0} = -\frac{1}{2}, \quad \lim_{s \rightarrow \infty} \frac{d}{ds} h_{\kappa}(g^{-1}(s)) = \frac{1}{2}, \quad (59)$$

$s \mapsto h_{\kappa}(g^{-1}(s))$ has a unique local minimum, which is also the global minimum. If s_{κ} is the minimizer, $h_{\kappa}(g^{-1}(s))$ is strictly decreasing for $0 \leq s \leq s_{\kappa}$ and strictly increasing for $s \geq s_{\kappa}$. Since g is strictly increasing, $h_{\kappa}(x)$ attains its global minimum in $x = E_{\kappa} = g^{-1}(s_{\kappa})$, is strictly decreasing for $0 \leq x \leq E_{\kappa}$ and strictly increasing for $x \geq E_{\kappa}$. Therefore,

$$\min_{x \in [0,E]} h_{\kappa}(x) = \begin{cases} h_{\kappa}(E), & 0 \leq E \leq E_{\kappa} \\ h_{\kappa}(E_{\kappa}), & E \geq E_{\kappa} \end{cases}. \quad (60)$$

Proof. Let $\rho_{A_1^n B_1^n R}$ be a classical extension of $(\rho_{AB}^{\kappa,E})^{\otimes n}$, where $A_1^n = A_1 \dots A_n$ and analogously for B_1^n . The quantum state $U_{\kappa}^{\dagger \otimes n} \rho_{A_1^n B_1^n R} U_{\kappa}^{\otimes n}$ is a classical extension of $\omega_A(E)^{\otimes n} \otimes |0\rangle_B \langle 0|^{\otimes n}$, therefore it has the form $\omega_{A_1^n R} \otimes |0\rangle_B \langle 0|^{\otimes n}$ for some quantum-classical state $\omega_{A_1^n R}$ that is a classical extension of $\omega_A(E)^{\otimes n}$. The quantum-classical state $\rho_{A_1^n B_1^n R}$ has then the form

$$\rho_{A_1^n B_1^n R} = U_{\kappa}^{\otimes n} \left(\omega_{A_1^n R} \otimes |0\rangle_B \langle 0|^{\otimes n} \right) U_{\kappa}^{\dagger \otimes n}, \quad \int_{\mathcal{R}} \omega_{A_1^n |R=r} d\rho_R(r) = \omega_A(E)^{\otimes n}. \quad (61)$$

Conversely, any state of the form (61) is a classical extension of $\rho_{AB}^{\kappa,E}$. We have for any $r \in \mathcal{R}$

$$\begin{aligned}\rho_{A_1^n B_1^n | R=r} &= U_{\kappa}^{\otimes n} \left(\omega_{A_1^n | R=r} \otimes |0\rangle_B \langle 0|^{\otimes n} \right) U_{\kappa}^{\dagger \otimes n}, \\ \text{Tr}_{B_1^n} \rho_{A_1^n B_1^n | R=r} &= \mathcal{A}_{\kappa}^{\otimes n}(\omega_{A_1^n | R=r}), \\ \text{Tr}_{A_1^n} \rho_{A_1^n B_1^n | R=r} &= \tilde{\mathcal{A}}_{\kappa}^{\otimes n}(\omega_{A_1^n | R=r}),\end{aligned}\tag{62}$$

where $\tilde{\mathcal{A}}_{\kappa}$ is the complementary channel of \mathcal{A}_{κ} ¹¹. Then,

$$\begin{aligned}I(A_1^n; B_1^n | R)_{\rho_{A_1^n B_1^n}} &= \int_{\mathcal{R}} I(A_1^n; B_1^n)_{\rho_{A_1^n B_1^n | R=r}} d\rho_R(r) \\ &= \int_{\mathcal{R}} \left(S\left(\mathcal{A}_{\kappa}^{\otimes n}(\omega_{A_1^n | R=r})\right) + S\left(\tilde{\mathcal{A}}_{\kappa}^{\otimes n}(\omega_{A_1^n | R=r})\right) - S(\omega_{A_1^n | R=r}) \right) d\rho_R(r).\end{aligned}\tag{63}$$

a. Upper bound Let $n = 1$ and let $E' \in [0, E]$. Choosing $\mathcal{R} = \mathbb{C}$, we have

$$\omega(E) = \int_{\mathbb{C}} D_r \omega(E') D_r^{\dagger} e^{-\frac{|r|^2}{E-E'}} \frac{dr}{\pi},\tag{64}$$

where for any $r \in \mathbb{C}$, D_r is the unitary operator that displaces by r the ladder operator¹¹:

$$D_r^{\dagger} a D_r = a + r \mathbb{I}.\tag{65}$$

We can then choose $\omega_{A|R=r} = \omega(E')$ for any $r \in \mathbb{C}$. Since

$$\mathcal{A}_{\kappa}(\omega(E')) = \omega(\kappa E' + \kappa - 1), \quad \tilde{\mathcal{A}}_{\kappa}(\omega(E')) = \omega((\kappa - 1)(E' + 1)),\tag{66}$$

we have from (63)

$$E_{\text{sq,c}}^{\infty} \left(\rho_{AB}^{\kappa,E} \right) \leq E_{\text{sq,c}} \left(\rho_{AB}^{\kappa,E} \right) \leq \frac{1}{2} I(A; B | R)_{\rho_{ABR}} = \frac{1}{2} h_{\kappa}(E'),\tag{67}$$

and the claim follows taking the minimum of the right-hand side of (67) over $E' \in [0, E]$.

b. Lower bound $\mathbf{E}_{\text{sq,c}}$: Let $n = 1$. Theorem 4 and Theorem 5 imply for any $r \in \mathcal{R}$

$$S\left(\mathcal{A}_{\kappa}(\omega_{A|R=r})\right) + S\left(\tilde{\mathcal{A}}_{\kappa}(\omega_{A|R=r})\right) - S(\omega_{A|R=r}) \geq h_{\kappa}(g^{-1}(S(\omega_{A|R=r}))).\tag{68}$$

From [79, Lemma 15], the function $s \mapsto h_{\kappa}(g^{-1}(s))$ is convex. We then have from (63), (68) and Jensen's inequality

$$\begin{aligned}I(A; B | R)_{\rho_{ABR}} &\geq \int_{\mathcal{R}} h_{\kappa}(g^{-1}(S(\omega_{A|R=r}))) d\rho_R(r) \geq h_{\kappa}(g^{-1}(S(A|R)_{\omega_{AR}})) \\ &\geq \inf_{E' \in [0, E]} h_{\kappa}(E'),\end{aligned}\tag{69}$$

where we have used that $0 \leq g^{-1}(S(A|R)_{\omega_{AR}}) \leq E$ since g^{-1} is increasing and

$$0 \leq \int_{\mathcal{R}} S(\omega_{A|R=r}) d\rho_R(r) = S(A|R)_{\omega_{AR}} \leq S(A)_{\omega_{AR}} = g(E). \quad (70)$$

Finally, taking the infimum of the left-hand side of (69) over all the classical extensions ρ_{ABR} of $\rho_{AB}^{\kappa,E}$ we get

$$E_{\text{sq,c}}(\rho_{AB}^{\kappa,E}) \geq \frac{1}{2} \inf_{E' \in [0,E]} h_{\kappa}(E'). \quad (71)$$

$E_{\text{sq,c}}^{\infty}$: The proof with generic n is analogous to the proof for $n = 1$: Conjecture 1 and Theorem 5 imply for any $r \in \mathcal{R}$

$$\begin{aligned} & S\left(\mathcal{A}_{\kappa}^{\otimes n}(\omega_{A_1^n|R=r})\right) + S\left(\tilde{\mathcal{A}}_{\kappa}^{\otimes n}(\omega_{A_1^n|R=r})\right) - S(\omega_{A_1^n|R=r}) \\ & \geq n h_{\kappa}\left(g^{-1}\left(\frac{1}{n}S(\omega_{A_1^n|R=r})\right)\right). \end{aligned} \quad (72)$$

We then have from (63), (72) and Jensen's inequality

$$\begin{aligned} I(A_1^n; B_1^n | R)_{\rho_{A_1^n B_1^n R}} & \geq n \int_{\mathcal{R}} h_{\kappa}\left(g^{-1}\left(\frac{1}{n}S(\omega_{A_1^n|R=r})\right)\right) d\rho_R(r) \\ & \geq n h_{\kappa}\left(g^{-1}\left(\frac{1}{n}S(A_1^n | R)_{\omega_{A_1^n R}}\right)\right) \geq n \inf_{E' \in [0,E]} h_{\kappa}(E'), \end{aligned} \quad (73)$$

where we have used that $0 \leq g^{-1}\left(\frac{1}{n}S(A_1^n | R)_{\omega_{A_1^n R}}\right) \leq E$ since g^{-1} is increasing and

$$0 \leq \int_{\mathcal{R}} S(\omega_{A_1^n|R=r}) d\rho_R(r) = S(A_1^n | R)_{\omega_{A_1^n R}} \leq S(A_1^n)_{\omega_{A_1^n R}} = n g(E). \quad (74)$$

Taking the infimum of the left-hand side of (73) over all the classical extensions $\rho_{A_1^n B_1^n R}$ of $\rho_{A_1^n B_1^n}^{\kappa,E}$ we get

$$E_{\text{sq,c}}(\rho_{AB}^{\kappa,E \otimes n}) \geq \frac{n}{2} \inf_{E' \in [0,E]} h_{\kappa}(E'), \quad (75)$$

and finally

$$E_{\text{sq,c}}^{\infty}(\rho_{AB}^{\kappa,E}) = \lim_{n \rightarrow \infty} \frac{1}{n} E_{\text{sq,c}}(\rho_{AB}^{\kappa,E \otimes n}) \geq \frac{1}{2} \inf_{E' \in [0,E]} h_{\kappa}(E'). \quad (76)$$

c. Separation between squashed entanglement and classical squashed entanglement From the upper bound of (22) and Remark 2, it is sufficient to prove that for any $\kappa > 1$,

$$g\left(\left(\kappa - \frac{1}{2}\right)E + \kappa - 1\right) - g\left(\frac{E}{2}\right) < \frac{1}{2} \begin{cases} h_{\kappa}(E), & 0 < E \leq E_{\kappa} \\ h_{\kappa}(E_{\kappa}), & E \geq E_{\kappa} \end{cases}. \quad (77)$$

Let us consider the case $0 < E \leq E_{\kappa}$. The claim is equivalent to

$$2g\left(\left(\kappa - \frac{1}{2}\right)E + \kappa - 1\right) - g(\kappa E + \kappa - 1) - g((\kappa - 1)(E + 1)) < 2g\left(\frac{E}{2}\right) - g(E). \quad (78)$$

For $\kappa = 1$, equality holds in (78). The derivative with respect to κ of the left-hand side of (78) is

$$2(E+1) \left(g' \left((\kappa - \frac{1}{2})E + \kappa - 1 \right) - \frac{g'(\kappa E + \kappa - 1) + g'((\kappa - 1)(E + 1))}{2} \right),$$

and is strictly negative since g' is strictly convex, hence the claim follows.

For $E \geq E_\kappa$, the claim follows since

$$\begin{aligned} g \left((\kappa - \frac{1}{2})E + \kappa - 1 \right) - g \left(\frac{E}{2} \right) &\leq g \left((\kappa - \frac{1}{2})E_\kappa + \kappa - 1 \right) - g \left(\frac{E_\kappa}{2} \right) \\ &< \frac{1}{2} h_\kappa(E_\kappa). \end{aligned} \tag{79}$$

□

V. CONCLUSIONS AND OPEN PROBLEMS


We have determined the maximum squashed entanglement achievable between sender and receiver of the noiseless quantum Gaussian attenuator and amplifier (Theorem 2), and proved that it is strictly larger than the corresponding secret key capacity. This result opens the way to determine the squashed entanglement of the noisy quantum Gaussian attenuators and amplifiers, for which only upper bounds are known^{24,31–33}.

Our proof is based on a new lower bound to the squashed entanglement of the quantum Gaussian state (21) obtained applying a two-mode squeezing operation to a quantum thermal Gaussian state tensored with the vacuum state (Theorem 1). Despite being extremely tight, the lower bound is optimal only in the limit of infinite average energy. Therefore, determining the exact value of the squashed entanglement of the quantum Gaussian state (21) for finite average energy is still an open problem. We conjecture that this squashed entanglement coincides with the upper bound of Theorem 1, which is achieved by a Gaussian extension of the state. Furthermore, we conjecture that the squashed entanglement of any quantum Gaussian state is achieved by a Gaussian extension.

We have also determined the classical squashed entanglement of the quantum Gaussian state (21), and proved that it is achieved by a classical Gaussian extension of the state. This is the first time that the classical squashed entanglement of a quantum Gaussian state is determined. Therefore, our result opens the way to determine the classical squashed entanglement of all quantum Gaussian states, which we conjecture to be always achieved by a classical Gaussian extension.

ACKNOWLEDGMENTS

We thank Matthias Christandl for fruitful discussions and Stefano Pirandola and Mark M. Wilde for useful comments.

 This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 792557.

We acknowledge support from the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union’s Horizon 2020 Programme (QuantAlgo project) via the Innovation Fund Denmark.

Appendix A: Entropic inequalities

A longstanding conjecture in quantum communication theory states that pairs of n -mode thermal quantum Gaussian states minimize the output entropy of the beam-splitter and the squeezing operation among all the pairs of n -mode input states with assigned entropies⁸². This conjecture was first formulated in 2007 to determine the maximum rates for classical communication to two receivers with the noiseless quantum Gaussian broadcast channel^{66–69}. A fundamental step towards the proof of the conjecture has been the proof of the quantum Entropy Power Inequality^{70–73,78}, which provides an almost optimal lower bound to the output entropy of the beam-splitter and the squeezing. The constrained minimum output entropy conjecture has then been proved for $n = 1$ in the special case when one of the two input states of the beam-splitter or of the squeezing operation is Gaussian, and therefore the quantum channel that maps the input to the output is a quantum Gaussian attenuator, amplifier or phase-contravariant channel^{74–77,80,81}. In this paper we exploit the constrained minimum output entropy conjecture for the noiseless quantum Gaussian amplifier:

Theorem 4 (one-mode constrained minimum output entropy conjecture⁷⁷). *Quantum thermal Gaussian input states minimize the output entropy of the one-mode noiseless quantum Gaussian amplifier among all the input states with a given entropy. In other words, for any one-mode quantum state ρ , let*

$$\omega_\rho = \omega(g^{-1}(S(\rho))) \tag{A1}$$

be the one-mode quantum thermal Gaussian state as in (7) with the same entropy as ρ . Then, for

any $\kappa \geq 1$

$$S(\mathcal{A}_\kappa(\rho)) \geq S(\mathcal{A}_\kappa(\omega_\rho)) = g(\kappa g^{-1}(S(\rho)) + \kappa - 1). \quad (\text{A2})$$

For $n \geq 2$, the constrained minimum output entropy conjecture is still open in general, and has been proved only for the quantum Gaussian channels that are entanglement breaking^{79,83}, which include the complementary channel of the noiseless quantum Gaussian amplifier:

Conjecture 1 (minimum output entropy conjecture [82, Conjecture V.1]). *For any $n \in \mathbb{N}$, quantum thermal Gaussian input states minimize the output entropy of the n -mode Gaussian quantum-limited amplifier among all the input states with a given entropy. In other words, for any n -mode quantum state ρ , let*

$$\omega_\rho = \omega(g^{-1}(\frac{1}{n}S(\rho)))^{\otimes n} \quad (\text{A3})$$

be the n -mode quantum thermal Gaussian state with the same entropy as ρ . Then, for any $\kappa \geq 1$

$$S(\mathcal{A}_\kappa^{\otimes n}(\rho)) \geq S(\mathcal{A}_\kappa^{\otimes n}(\omega_\rho)) = ng(\kappa g^{-1}(\frac{1}{n}S(\rho)) + \kappa - 1). \quad (\text{A4})$$

Remark 3. Conjecture 1 has been proved in the particular case when the input state ρ is pure⁸⁸⁻⁹¹.

Theorem 5 ([83, Corollary 5]). *For any $n \in \mathbb{N}$, quantum thermal Gaussian input states minimize the output entropy of the complementary channel of the n -mode noiseless quantum Gaussian amplifier among all the input states with a given entropy. In other words, for any n -mode quantum state ρ , let*

$$\omega_\rho = \omega(g^{-1}(\frac{1}{n}S(\rho)))^{\otimes n} \quad (\text{A5})$$

be the n -mode quantum thermal Gaussian state with the same entropy as ρ . Then, for any $\kappa \geq 1$

$$S(\tilde{\mathcal{A}}_\kappa^{\otimes n}(\rho)) \geq S(\tilde{\mathcal{A}}_\kappa^{\otimes n}(\omega_\rho)) = ng((\kappa - 1)(g^{-1}(\frac{1}{n}S(\rho)) + 1)). \quad (\text{A6})$$

A conditional version of the quantum Entropy Power Inequality has been proved, where all the entropies are conditioned on an external quantum system²⁷⁻²⁹. In this paper, we exploit its version for the two-mode squeezing operation:

Theorem 6 (quantum conditional Entropy Power Inequality²⁸). *Let A be a one-mode Gaussian quantum system and let R be a generic quantum system. Let γ_{AR} be a joint quantum state on AR such that its marginal γ_A on A has finite average energy and its marginal γ_R on R has finite entropy.*

Let

$$\rho_{ABR} = U_\kappa(\gamma_{AR} \otimes |0\rangle_B\langle 0|)U_\kappa^\dagger, \quad (\text{A7})$$

where $|0\rangle_B$ is the vacuum state of B and U_κ is the two-mode squeezing operator defined in (17). Then,

$$\begin{aligned} S(A|R)_{\rho_{ABR}} &\geq \ln(\kappa \exp S(A|R)_{\gamma_{AR}} + \kappa - 1), \\ S(B|R)_{\rho_{ABR}} &\geq \ln((\kappa - 1) \exp S(A|R)_{\gamma_{AR}} + \kappa). \end{aligned} \quad (\text{A8})$$

Appendix B

Lemma 1. For any $E \geq 0$ and $\kappa \geq 1$, the function $\psi_{E,\kappa}$ is convex.

Proof. We have

$$\psi''_{E,\kappa}(\eta) = \frac{E(E+1)(\kappa-1)((\kappa+1-2\eta)E+\kappa)}{(1-\eta)((\kappa-\eta)E+\kappa-1)((\kappa-\eta)E+\kappa)((1-\eta)E+1)} \geq 0. \quad (\text{B1})$$

□

REFERENCES

- ¹R. R. Tucci, arXiv preprint quant-ph/9909041 (1999).
- ²R. R. Tucci, arXiv preprint quant-ph/0005119 (2000).
- ³R. R. Tucci, arXiv preprint quant-ph/0010041 (2000).
- ⁴R. R. Tucci, arXiv preprint quant-ph/0101123 (2001).
- ⁵R. R. Tucci, arXiv preprint quant-ph/0103040 (2001).
- ⁶R. R. Tucci, arXiv preprint quant-ph/0202144 (2002).
- ⁷M. Christandl and A. Winter, *Journal of mathematical physics* **45**, 829 (2004).
- ⁸F. G. Brandao, M. Christandl, and J. Yard, *Communications in Mathematical Physics* **306**, 805 (2011).
- ⁹K. P. Seshadreesan, M. Berta, and M. M. Wilde, *Journal of Physics A: Mathematical and Theoretical* **48**, 395303 (2015).
- ¹⁰M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2017).
- ¹¹A. S. Holevo, *Quantum Systems, Channels, Information: A Mathematical Introduction*, De Gruyter Studies in Mathematical Physics (De Gruyter, 2013).
- ¹²M. Tomamichel, *Quantum Information Processing with Finite Resources: Mathematical Foundations*, SpringerBriefs in Mathematical Physics (Springer International Publishing, 2015).

- ¹³K. Audenaert, J. Eisert, E. Jané, M. B. Plenio, S. Virmani, and B. De Moor, *Physical review letters* **87**, 217902 (2001).
- ¹⁴V. Vedral, *Reviews of Modern Physics* **74**, 197 (2002).
- ¹⁵M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, in *Theory of Cryptography Conference* (Springer, 2007) pp. 456–478.
- ¹⁶K. Li and A. Winter, *Communications in Mathematical Physics* **326**, 63 (2014).
- ¹⁷M. M. Wilde, *Quantum Information Processing* **15**, 4563 (2016).
- ¹⁸K. P. Seshadreesan and M. M. Wilde, *Physical Review A* **92**, 042321 (2015).
- ¹⁹K. Li and A. Winter, *Foundations of Physics* **48**, 910 (2018).
- ²⁰G. Adesso, M. Ericsson, and F. Illuminati, *Physical Review A* **76**, 022315 (2007).
- ²¹D. Avis, P. Hayden, and I. Savov, *Journal of Physics A: Mathematical and Theoretical* **41**, 115301 (2008).
- ²²D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song, *IEEE Transactions on Information Theory* **55**, 3375 (2009).
- ²³S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Nature communications* **8**, 15043 (2017).
- ²⁴M. Takeoka, S. Guha, and M. M. Wilde, *IEEE Transactions on Information Theory* **60**, 4987 (2014).
- ²⁵M. Berta and M. M. Wilde, *New Journal of Physics* **20**, 053044 (2018).
- ²⁶L. Lami, C. Hirche, G. Adesso, and A. Winter, *IEEE Transactions on Information Theory* **63**, 7553 (2017).
- ²⁷R. König, *Journal of Mathematical Physics* **56**, 022201 (2015).
- ²⁸G. De Palma and D. Trevisan, *Communications in Mathematical Physics* **360**, 639 (2018).
- ²⁹G. De Palma and S. Huber, *Journal of Mathematical Physics* **59**, 122201 (2018).
- ³⁰G. De Palma, *Journal of Physics A: Mathematical and Theoretical* (2019).
- ³¹M. Takeoka, S. Guha, and M. M. Wilde, *Nature communications* **5**, 5235 (2014).
- ³²K. Goodenough, D. Elkouss, and S. Wehner, *New Journal of Physics* **18**, 063005 (2016).
- ³³N. Davis, M. E. Shirokov, and M. M. Wilde, *Physical Review A* **97**, 062310 (2018).
- ³⁴F. Caruso, V. Giovannetti, and A. S. Holevo, *New Journal of Physics* **8**, 310 (2006).
- ³⁵F. Caruso and V. Giovannetti, *Physical Review A* **74**, 062307 (2006).
- ³⁶A. S. Holevo, *Problems of Information Transmission* **43**, 1 (2007).
- ³⁷C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and

- S. Lloyd, *Reviews of Modern Physics* **84**, 621 (2012).
- ³⁸A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, 2017).
- ³⁹C. H. Bennett and G. Brassard, “Proceedings of the IEEE international conference on computers, systems and signal processing,” (1984).
- ⁴⁰A. K. Ekert, *Physical review letters* **67**, 661 (1991).
- ⁴¹N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Reviews of modern physics* **74**, 145 (2002).
- ⁴²S. Lloyd, J. H. Shapiro, F. N. Wong, P. Kumar, S. M. Shahriar, and H. P. Yuen, *ACM SIGCOMM Computer Communication Review* **34**, 9 (2004).
- ⁴³S. L. Braunstein and P. Van Loock, *Reviews of Modern Physics* **77**, 513 (2005).
- ⁴⁴H. J. Kimble, *Nature* **453**, 1023 (2008).
- ⁴⁵V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Reviews of modern physics* **81**, 1301 (2009).
- ⁴⁶S. Pirandola and S. L. Braunstein, *Nature News* **532**, 169 (2016).
- ⁴⁷S. Pirandola, arXiv preprint arXiv:1601.00966 (2016).
- ⁴⁸K. Azuma, A. Mizutani, and H.-K. Lo, *Nature communications* **7**, 13523 (2016).
- ⁴⁹R. Laurenza and S. Pirandola, *Physical Review A* **96**, 032318 (2017).
- ⁵⁰R. Laurenza, S. L. Braunstein, and S. Pirandola, *Scientific reports* **8**, 15267 (2018).
- ⁵¹T. P. Cope, K. Goodenough, and S. Pirandola, *Journal of Physics A: Mathematical and Theoretical* **51**, 494001 (2018).
- ⁵²S. Wehner, D. Elkouss, and R. Hanson, *Science* **362**, eaam9288 (2018).
- ⁵³R. Laurenza, S. Tserkis, L. Banchi, S. L. Braunstein, T. C. Ralph, and S. Pirandola, *Physical Review A* **100**, 042301 (2019).
- ⁵⁴S. Pirandola, *Communications Physics* **2**, 51 (2019).
- ⁵⁵S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, arXiv preprint arXiv:1906.01645 (2019).
- ⁵⁶S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, *Physical review letters* **102**, 050503 (2009).
- ⁵⁷M. M. Wilde, M. Tomamichel, and M. Berta, *IEEE Transactions on Information Theory* **63**, 1792 (2017).
- ⁵⁸S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. Cope, G. Spedalieri, and L. Banchi, *Quantum Science and Technology* **3**, 035009 (2018).

- ⁵⁹M. Christandl and A. Müller-Hermes, *Communications in Mathematical Physics* **353**, 821 (2017).
- ⁶⁰F. G. Brandao, *Entanglement theory and the quantum simulation of many-body physics*, Ph.D. thesis, Imperial College London (2008).
- ⁶¹D. Yang, M. Horodecki, and Z. Wang, arXiv preprint quant-ph/0701149 (2007).
- ⁶²D. Yang, M. Horodecki, and Z. Wang, *Physical review letters* **101**, 140501 (2008).
- ⁶³W. Song, *International Journal of Theoretical Physics* **48**, 2191 (2009).
- ⁶⁴Y. Huang, *New journal of physics* **16**, 033027 (2014).
- ⁶⁵E. Wakakuwa, arXiv preprint arXiv:1904.08852 (2019).
- ⁶⁶S. Guha, J. H. Shapiro, and B. I. Erkmen, *Physical Review A* **76**, 032303 (2007).
- ⁶⁷S. Guha and J. H. Shapiro, in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on* (IEEE, 2007) pp. 1896–1900.
- ⁶⁸S. Guha, B. Erkmen, and J. H. Shapiro, in *Information Theory and Applications Workshop, 2008* (IEEE, 2008) pp. 128–130.
- ⁶⁹S. Guha, J. H. Shapiro, and B. Erkmen, in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on* (IEEE, 2008) pp. 91–95.
- ⁷⁰R. König and G. Smith, *IEEE Transactions on Information Theory* **60**, 1536 (2014).
- ⁷¹R. König and G. Smith, *IEEE Transactions on Information Theory* **62**, 4358 (2016).
- ⁷²G. De Palma, A. Mari, and V. Giovannetti, *Nature Photonics* **8**, 958 (2014).
- ⁷³G. De Palma, A. Mari, S. Lloyd, and V. Giovannetti, *Physical Review A* **91**, 032320 (2015).
- ⁷⁴G. De Palma, D. Trevisan, and V. Giovannetti, *IEEE Transactions on Information Theory* **62**, 2895 (2016).
- ⁷⁵G. De Palma, A. Mari, S. Lloyd, and V. Giovannetti, *Physical Review A* **93**, 062328 (2016).
- ⁷⁶G. De Palma, D. Trevisan, and V. Giovannetti, *IEEE Transactions on Information Theory* **63**, 728 (2017).
- ⁷⁷G. De Palma, D. Trevisan, and V. Giovannetti, *Physical Review Letters* **118**, 160503 (2017).
- ⁷⁸G. De Palma, *Gaussian optimizers and other topics in quantum information*, Ph.D. thesis, Scuola Normale Superiore, Pisa (Italy) (2016), supervisor: Prof. Vittorio Giovannetti; arXiv:1710.09395.
- ⁷⁹G. De Palma, D. Trevisan, and V. Giovannetti, arXiv preprint arXiv:1705.00499 (2017).
- ⁸⁰H. Qi, M. M. Wilde, and S. Guha, arXiv preprint arXiv:1607.05262 (2017).
- ⁸¹G. De Palma, D. Trevisan, and V. Giovannetti, *Annales Henri Poincaré* **19**, 2919 (2018).

- ⁸²G. De Palma, D. Trevisan, V. Giovannetti, and L. Ambrosio, *Journal of Mathematical Physics* **59**, 081101 (2018).
- ⁸³G. De Palma, *IEEE Transactions on Information Theory* **65**, 5959 (2019).
- ⁸⁴L. Bombelli, R. K. Koul, J. Lee, and R. D. Sorkin, *Physical Review D* **34**, 373 (1986).
- ⁸⁵A. Ferraro, S. Olivares, and M. Paris, *Gaussian States in Quantum Information*, Napoli series on physics and astrophysics (Bibliopolis, 2005).
- ⁸⁶S. Barnett and P. Radmore, *Methods in Theoretical Quantum Optics*, Oxford Series in Optical and Imaging Sciences (Clarendon Press, 2002).
- ⁸⁷M. M. Wolf, G. Giedke, and J. I. Cirac, *Physical Review Letters* **96**, 080502 (2006).
- ⁸⁸V. Giovannetti, A. Holevo, and R. García-Patrón, *Communications in Mathematical Physics* **334**, 1553 (2015).
- ⁸⁹A. S. Holevo, *Russian Mathematical Surveys* **70**, 331 (2015).
- ⁹⁰V. Giovannetti, A. S. Holevo, and A. Mari, *Theoretical and Mathematical Physics* **182**, 284 (2015).
- ⁹¹V. Giovannetti, R. García-Patrón, N. Cerf, and A. Holevo, *Nature Photonics* **8**, 796 (2014).