nature photonics

Supplementary information https://doi.org/10.1038/s41566-024-01595-9

Maximum tolerable excess noise in continuous-variable quantum key distribution and improved lower bound on two-way capacities

In the format provided by the authors and unedited

Supplementary Information: Maximum tolerable excess noise in CV-QKD and improved lower bound on two-way capacities

CONTENTS

I. NOTATION AND PRELIMINARIES

Let $\mathfrak{S}(\mathcal{H})$ be the set of quantum states on a Hilbert space $\mathcal{H}$. The trace norm of a bounded linear operator Θ is defined by $\|\Theta\|_1 := \operatorname{Tr}\sqrt{\Theta^\dagger\Theta}$. The von Neumann entropy of a quantum state ρ is denoted by $S(\rho) := -\operatorname{Tr}[\rho\log_2\rho]$. Let $\mathcal{H}_2$ be a bi-dimensional Hilbert space and let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis. For all $i,j\in\{0,1\}$, the state $|\psi_{ij}\rangle_{AB}\in\mathcal{H}_2^{(A)}\otimes\mathcal{H}_2^{(B)}$ is defined as

$$|\psi_{ij}\rangle_{AB} := \frac{1}{\sqrt{2}}\sum_{m=0}^{1}(-1)^{im}|m\rangle_A\otimes|m\oplus j\rangle_B\,, \tag{S1}$$

and is called a Bell state (or maximally entangled state), where $\oplus$ denotes the modulo 2 addition.

A. Gaussian quantum information

Let us briefly review the formalism of Gaussian quantum information [1]. We consider m-modes of harmonic oscillators S_1, S_2, ..., S_m, which are associated with the Hilbert space $L^2(\mathbb{R}^m)$ of square integrable functions. Each of these modes represents a single-mode of electromagnetic radiation with definite frequency and polarisation. For all $j = 1,2,\ldots,m$ the annihilation operator a_j of the mode S_i is defined as $a_j := \frac{\hat{x}_j+i\hat{p}_j}{\sqrt{2}}$, where $\hat{x}_j$ and $\hat{p}_j$ are the well-known position and momentum operators of S_j. The operator $a_j^\dagger a_j$ is called the photon number of the mode S_j. The nth

Fock state of the mode S_j is denoted by $|n\rangle_{S_j}$. By defining the so-called quadrature vector $\hat{\mathbf{R}} := (\hat{x}_1, \hat{p}_1, ..., \hat{x}_m, \hat{p}_m)^\intercal$, one can write the canonical commutation relations as $[\hat{\mathbf{R}}, \hat{\mathbf{R}}^\intercal] = i\,\Omega_m$, where $\Omega_m := \mathbb{1}_m \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\mathbb{1}_m$ is the $m \times m$ identity matrix. The characteristic function $\chi_\rho : \mathbb{R}^{2m} \to \mathbb{C}$ of a state $\rho \in \mathfrak{S}(L^2(\mathbb{R}^m))$ is defined as $\chi_\rho(\mathbf{r}) = \mathrm{Tr}[\rho D_{-\mathbf{r}}]$, where for all $\mathbf{r} \in \mathbb{R}^{2m}$ the displacement operator $D_\mathbf{r}$ is defined as

$$D_\mathbf{r} := e^{i\mathbf{r}^\intercal \Omega_m \hat{\mathbf{R}}}\,. \tag{S2}$$

Any state ρ can be written in terms of its characteristic function as

$$\rho = \int_{\mathbb{R}^{2m}} \frac{\mathrm{d}^{2m}\mathbf{r}}{(2\pi)^m} \chi_\rho(\mathbf{r}) D_\mathbf{r} \tag{S3}$$

and hence quantum states and characteristic functions are in one-to-one correspondence. The first moment and the covariance matrix of a quantum state ρ are defined as

$$\mathbf{m}(\rho) = \mathrm{Tr}\left[\hat{\mathbf{R}}\,\rho\right]\,, \tag{S4}$$

$$V(\rho) = \mathrm{Tr}\left[\left\{(\hat{\mathbf{R}} - \mathbf{m}(\rho)), (\hat{\mathbf{R}} - \mathbf{m}(\rho))^\intercal\right\}\rho\right]\,, \tag{S5}$$

respectively, where $\{A, B\} := AB + BA$ is the anti-commutator. Note that the covariance matrix is defined with respect an ordering of the modes in the definition of the quadrature vector: here such an ordering is $(S_1, S_2, \dots, S_m)$. A state ρ is said to be Gaussian if there exists a $2m \times 2m$ real positive definite matrix H_ρ and a vector $\mathbf{m}_\rho \in \mathbb{R}^{2m}$ such that ρ can be written as a ground or a thermal state of the Hamiltonian $\frac{1}{2}(\hat{\mathbf{R}} - \mathbf{m}_\rho)^\intercal H(\hat{\mathbf{R}} - \mathbf{m}_\rho)$, i.e.

$$\rho = \frac{e^{-\frac{1}{2}(\hat{\mathbf{R}} - \mathbf{m}_\rho)^\intercal H_\rho (\hat{\mathbf{R}} - \mathbf{m}_\rho)}}{\mathrm{Tr}\left[e^{-\frac{1}{2}(\hat{\mathbf{R}} - \mathbf{m}_\rho)^\intercal H_\rho (\hat{\mathbf{R}} - \mathbf{m}_\rho)}\right]}\,. \tag{S6}$$

It can be shown that $\mathbf{m}(\rho) = \mathbf{m}_\rho$ and $V(\rho) = V_\rho$, where $V_\rho := \coth\left(\frac{i\,\Omega_m H_\rho}{2}\right) i\,\Omega_m$. The characteristic function of a Gaussian state ρ is a Gaussian function in $\mathbf{r}$ which can be written in terms of $\mathbf{m}(\rho)$ and $V(\rho)$ as

$$\chi_\rho(\mathbf{r}) = \exp\left(-\frac{1}{4}(\Omega_m \mathbf{r})^\intercal V(\rho) \Omega_m \mathbf{r} + i(\Omega_m \mathbf{r})^\intercal \mathbf{m}(\rho)\right)\,. \tag{S7}$$

An example of Gaussian state is the thermal state $\tau_{N_s} := \frac{1}{N_s+1}\sum_{n=0}^\infty \left(\frac{N_s}{N_s+1}\right)^n |n\rangle\langle n|$, where the parameter $N_s \geq 0$ is its mean photon number ($N_s = \mathrm{Tr}[a^\dagger a\, \tau_{N_s}]$), which satisfies

$$\begin{aligned} \mathbf{m}(\tau_{N_s}) &= (0, 0)^\intercal\,, \\ V(\tau_{N_s}) &= (2N_S + 1)\mathbb{1}_2\,. \end{aligned} \tag{S8}$$

Another example of Gaussian state is the two-mode squeezed vacuum state $|\Psi_{N_s}\rangle_{S_1 S_2}$, which for all $N_s \geq 0$ it is defined as

$$|\Psi_{N_s}\rangle_{S_1 S_2} := \frac{1}{\sqrt{N_s + 1}} \sum_{n=0}^{\infty} \left(\frac{N_s}{N_s + 1}\right)^{n/2} |n\rangle_{S_1} |n\rangle_{S_2}\,, \tag{S9}$$

where N_s denotes the mean photon number of the mode S_1 (or, equivalently, of the mode S_2), i.e.

$$N_s = \mathrm{Tr}_{S_2}[a_1^\dagger a_1\, |\Psi_{N_s}\rangle\langle\Psi_{N_s}|_{S_1 S_2}]\,. \tag{S10}$$

The first moment and covariance matrix of $|\Psi_{N_s}\rangle_{S_1 S_2}$ are

$$\begin{aligned} \mathbf{m}(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|) &= (0, 0, 0, 0)^\mathrm{T}\,, \\ V(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|) &= \begin{pmatrix} (2N_s + 1)\mathbb{1}_2 & 2\sqrt{N_s(N_s + 1)}\sigma_z \\ 2\sqrt{N_s(N_s + 1)}\sigma_z & (2N_s + 1)\mathbb{1}_2 \end{pmatrix}\,, \end{aligned} \tag{S11}$$

where $\mathbb{1}_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

A quantum channel is said to be Gaussian if it maps Gaussian states into Gaussian states. Later we will focus on three important examples of Gaussian quantum channels: the thermal attenuator, the thermal amplifier, and the additive Gaussian noise. Before concluding this brief recap of Gaussian quantum information, let us state a lemma which will be useful in the following. The forthcoming Lemma S1 provides a necessary and sufficient condition on the covariance matrix to assess whether a two-mode Gaussian state is entangled [1, 2]. This condition is based on the fact that a two-mode Gaussian states is separable (not entangled) if and only if it is PPT [1, 2].

Lemma S1 [1, 2]**.** *Let $\rho \in \mathfrak{S}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$ be a two-mode Gaussian state. Let us write its covariance matrix $V(\rho)$ with respect the ordering (S_1, S_2) as*

$$V(\rho) = \begin{pmatrix} V_{S_1} & V_{S_1 S_2} \\ V_{S_1 S_2}^{\intercal} & V_{S_2} \end{pmatrix} \tag{S12}$$

and define the function $f : \mathfrak{S}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2}) \to \mathbb{R}$ as $f(\rho) := 1 + \det(V(\rho)) + 2\det(V_{S_1 S_2}) - \det(V_{S_1}) - \det(V_{S_2})$. The state ρ is entangled if and only if $f(\rho) < 0$.

The forthcoming Lemma S2 gives necessary and sufficient condition on a Gaussian quantum channel to be entanglement breaking [3, Chapter 4.6].

Lemma S2. *[4] Let $\Phi : \mathfrak{S}(L^2(\mathbb{R}^m)) \to \mathfrak{S}(L^2(\mathbb{R}^m))$ be a Gaussian quantum channel. Let $K, \beta \in \mathbb{R}^{2m\times 2m}$ and $l \in \mathbb{R}^{2m}$ such that for all $\rho \in \mathfrak{S}(L^2(\mathbb{R}^m))$ it holds that*

$$\begin{aligned} \mathbf{m}(\Phi(\rho)) &= K\,\mathbf{m}(\rho)\,, \\ V(\Phi(\rho)) &= K^{\intercal}\, V(\rho) K + \beta\,. \end{aligned} \tag{S13}$$

Then, Φ is entanglement breaking if and only if β admits the following decomposition:

$$\beta = \alpha + \gamma\,, \quad \textit{where } \alpha, \gamma \in \mathbb{R}^{2m\times 2m} \textit{ with } \alpha \geq i\,\Omega_m \textit{ and } \gamma \geq iK^{\intercal}\,\Omega_m K\,. \tag{S14}$$

B. Two-way capacities of a quantum channel

The two-way quantum capacity $Q_2(\Phi)$ and the secret-key capacity $K(\Phi)$ of a quantum channel Φ are the maximum achievable rate of qubits and secret-key bits, respectively, that can be reliably transmitted through Φ by assuming that the sender Alice and the receiver Bob have free access to a public, noiseless, two-way classical communication line. The rate of qubits (resp. secret-key bits) is defined as the ratio between the number of reliably transmitted qubits (resp. secret-key bits) and the number of uses of Φ [5, Chapters 14 and 15]. An ebit is a Bell state $|\psi_{00}\rangle_{AB}$ shared between Alice and Bob. For any Φ, the two-way capacities satisfy

$$Q_2(\Phi) \leq K(\Phi)\,. \tag{S15}$$

Indeed, by recalling that Alice and Bob can freely send an infinite amount of bits to each other, an ebit can generate a secret-key bit, thanks to E91 protocol [6], and hence $Q_2(\Phi) \leq K(\Phi)$. The two-way quantum capacity $Q_2(\Phi)$ and the secret-key capacity $K(\Phi)$ are collectively called the *two-way capacities of* Φ.

In practice, Alice has access to a limited budget (N_s) of energy to produce each input signal. Here, by definition, the energy of a signal initialised in a state ρ is equal to its mean photon number $\mathrm{Tr}[\rho\, a^\dagger a]$. Fixed $N_s > 0$, the energy-constrained (EC) two-way capacities $Q_2(\Phi, N_s)$ and $K(\Phi, N_s)$ are defined as above but the maximisation of the rate is restricted to the strategies such that the average photon number less or equal to N_s. In other words, N_s is the maximum allowed average photon number of the input signals to the channel Φ. In addition note that the generalisation of S15 to the EC case holds, i.e.

$$Q_2(\Phi, N_s) \leq K(\Phi, N_s)\,, \tag{S16}$$

and that any EC capacity is upper bounded by the corresponding unconstrained capacity and tends to it in the limit $N_s \to \infty$.

C. Entanglement distillation

The goal of an entanglement distillation protocol is to turn a large number n of copies of a bipartite entangled state $\rho_{AB} \in \mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ shared between Alice and Bob into a smaller number m of ebits by LOCCs (local operations and classical communication). The yield of an entanglement distillation protocol is defined by the ratio m/n. The two-way distillable entanglement $E_d(\rho_{AB})$ of ρ_{AB} is defined as the maximum yields over all the possible entanglement distillation protocols [7] [5, Chapter 8]. The state ρ_{AB} is said to be *distillable* if $E_d(\rho_{AB}) > 0$. The coherent information of ρ_{AB} is defined by

$$I_{\mathrm{c}}(\rho_{AB}) \coloneqq S(\mathrm{Tr}_A\, \rho_{AB}) - S(\rho_{AB}) \tag{S17}$$

and it is a yield achievable by an entanglement distillation protocol which requires classical communication only from Alice to Bob [8]. By exchanging the roles of Alice and Bob in such an entanglement distillation protocol, the reverse coherent information of ρ_{AB}, which is defined by

$$I_{\mathrm{rc}}(\rho_{AB}) \coloneqq S(\mathrm{Tr}_B\, \rho_{AB}) - S(\rho_{AB})\,, \tag{S18}$$

is a yield achievable by an entanglement distillation protocol which only requires classical communication only from Bob to Alice [8]. In particular, the following inequality, known as *hashing inequality*, holds:

$$E_d(\rho_{AB}) \geq \max\{I_{\mathrm{c}}(\rho_{AB})\,, I_{\mathrm{rc}}(\rho_{AB})\}\,. \tag{S19}$$

Let us briefly link the notions of distillable entanglement E_d and two-way quantum capacity $Q_2(\Phi, N_s)$. Suppose that Alice produces n copies of a state $\rho_{AA'}$ such that the mean photon number of the half A' is less or equal to N_s. Then, she uses n times the channel Φ to send the halves A', which satisfy the energy constraint, to Bob. Hence, n copies of $\mathrm{Id}_A \otimes \Phi(\rho_{AA'})$ are shared between Alice and Bob and can be used to generate ebits by means of an entanglement distillation protocol. Consequently, it holds that

$$Q_2(\Phi, N_s) \geq E_d\left(\mathrm{Id}_A \otimes \Phi(\rho_{AA'})\right) \tag{S20}$$

for all $N_s \geq 0$ and all $\rho_{A'A}$ satisfying $\mathrm{Tr}[a^\dagger a\, \rho_{A'A}] \leq N_s$, where a denotes the annihilation operator on A'.

If a bipartite state ρ_{AB} is such that the hashing inequality is trivial (i.e. the right-hand side of (S19) is negative), in order to obtain a non-trivial lower bound on $E_d(\rho_{AB})$, one can adopt a sufficiently large number of iterations of a *recurrence protocol* on ρ_{AB} prior to apply the hashing inequality. In the context of entanglement distillation, the goal of a recurrence protocol is to transform a certain number of copies of the state ρ_{AB} into fewer copies of another state ρ'_{AB} such that $\langle\psi_{00}|\, \rho'_{AB}\, |\psi_{00}\rangle > \langle\psi_{00}|\, \rho_{AB}\, |\psi_{00}\rangle$ [7, 9, 10]. Examples of recurrence protocols for qubits can be found in [10–12], and their generalisations to the case of qudits in [13–15]. In the present paper we will exploit the recently introduced P1-or-P2 recurrence protocol [16]. To achieve a nonzero yield, one may adopt a suitable number of iterations of a recurrence protocol and then apply the hashing or breeding protocol [9, 10]. The latter protocols, which exploit only one-way classical communication, achieves the yield of the hashing inequality in (S19). Improvements of the hashing and breeding protocols, which exploit two-way classical communication, have been provided in [17]: the two-way distillable entanglement of a convex combination of Bell states $\rho_{AB} \coloneqq \sum_{ij=0}^{1} \alpha_{ij}\, |\psi_{ij}\rangle\!\langle\psi_{ij}|$ is lower bounded by

$$Y(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}) \coloneqq \max\left(0, 1 - H(\{\alpha_{ij}\}) + \frac{1}{2}(\alpha_{00}+\alpha_{10})(\alpha_{11}+\alpha_{01})\left[H_2\left(\frac{\alpha_{00}}{\alpha_{00}+\alpha_{10}}\right) + H_2\left(\frac{\alpha_{11}}{\alpha_{01}+\alpha_{11}}\right)\right]\right), \tag{S21}$$

with $H(\{\alpha_{ij}\}) \coloneqq -\sum_{m,n=0}^{1} \alpha_{mn} \log_2 \alpha_{mn}$ being the Shannon entropy and $H_2(x) \coloneqq -x\log_2 x - (1-x)\log_2(1-x)$ for all $x \in [0,1]$ being the binary entropy. The yield in (S21) is larger than the yield achieved by the hashing protocol, which is $I_{\mathrm{c}}\left(\sum_{ij=0}^{1} \alpha_{ij}\, |\psi_{ij}\rangle\!\langle\psi_{ij}|\right) = 1 - H(\{\alpha_{ij}\})$. Protocols with larger yiels than (S21) may be obtained by exploiting the numerical methods introduced in [18].

Now, let us briefly review the definition, the relevant properties, and the known bounds on the two-way capacities of phase-insensitive bosonic Gaussian channels, namely thermal attenuator, thermal amplifier, and additive Gaussian noise.

D. Thermal attenuator

Let $\mathcal{H}_S$ and $\mathcal{H}_E$ be single-mode systems and let a and b denote their annihilation operators, respectively. For all $\lambda \in [0,1]$ and $\nu \geq 0$, a thermal attenuator $\mathscr{E}_{\lambda,\nu} : \mathfrak{S}(\mathcal{H}_S) \to \mathfrak{S}(\mathcal{H}_S)$ is a quantum channel defined by

$$\mathscr{E}_{\lambda,\nu}(\rho) \coloneqq \mathrm{Tr}_E\left[U_\lambda^{SE}\left(\rho^S \otimes \tau_\nu^E\right) U_\lambda^{SE\,\dagger}\right], \tag{S22}$$

where U_λ^{SE} denotes the unitary operator associated with a beam splitter of transmissivity λ, i.e.

$$U_\lambda^{SE} := \exp\left[\arccos\sqrt{\lambda}\left(a^\dagger b - a\, b^\dagger\right)\right]\,, \tag{S23}$$

and $\tau_\nu \in \mathfrak{S}(\mathcal{H}_E)$ denotes the thermal state with mean photon number equal to ν. The beam splitter unitary can be expressed via the following disentangling formula [19, Appendix 5]

$$U_\lambda^{SE} = e^{-\sqrt{\frac{1-\lambda}{\lambda}}ab^\dagger} e^{\frac{1}{2}\ln\lambda\left(a^\dagger a - b^\dagger b\right)} e^{\sqrt{\frac{1-\lambda}{\lambda}}a^\dagger b}\,. \tag{S24}$$

By writing the quadrature vector $\hat{\mathbf{R}}$ with respect the ordering (S,E), it can be shown that

$$\left(U_\lambda^{SE}\right)^\dagger \hat{\mathbf{R}}\, U_\lambda^{SE} = S_\lambda\, \hat{\mathbf{R}}\,, \tag{S25}$$

where

$$S_\lambda := \begin{pmatrix} \sqrt{\lambda}\,\mathbb{1}_2 & \sqrt{1-\lambda}\,\mathbb{1}_2 \\ -\sqrt{1-\lambda}\,\mathbb{1}_2 & \sqrt{\lambda}\,\mathbb{1}_2 \end{pmatrix}\,. \tag{S26}$$

This implies that for all $\sigma_{SE} \in \mathfrak{S}(\mathcal{H}_S \otimes H_E)$ it holds that

$$\begin{aligned} \mathbf{m}\left(U_\lambda^{SE}\sigma_{SE}\left(U_\lambda^{SE}\right)^\dagger\right) &= S_\lambda\,\mathbf{m}(\sigma_{SE})\,, \\ V\left(U_\lambda^{SE}\sigma_{SE}\left(U_\lambda^{SE}\right)^\dagger\right) &= S_\lambda\, V(\sigma_{SE})\, S_\lambda^\intercal\,. \end{aligned} \tag{S27}$$

In terms of the annihilation operators a and b, the transformation in (S25) reads

$$\begin{aligned} \left(U_\lambda^{SE}\right)^\dagger a\, U_\lambda^{SE} &= \sqrt{\lambda}\, a + \sqrt{1-\lambda}\, b\,, \\ U_\lambda^{SE} a\,\left(U_\lambda^{SE}\right)^\dagger &= \sqrt{\lambda}\, a - \sqrt{1-\lambda}\, b\,, \\ \left(U_\lambda^{SE}\right)^\dagger b\, U_\lambda^{SE} &= -\sqrt{1-\lambda}\, a + \sqrt{\lambda}\, b\,, \\ U_\lambda^{SE} b\,\left(U_\lambda^{SE}\right)^\dagger &= \sqrt{1-\lambda}\, a + \sqrt{\lambda}\, b\,. \end{aligned} \tag{S28}$$

It can be shown that for any single-mode state ρ it holds that

$$\begin{aligned} &\mathbf{m}\left(\mathscr{E}_{\lambda,\nu}(\rho)\right) = \sqrt{\lambda}\,\mathbf{m}(\rho)\,, \\ &V\left(\mathscr{E}_{\lambda,\nu}(\rho)\right) = \lambda\, V(\rho) + (1-\lambda)(2\nu+1)\mathbb{1}_2\,, \end{aligned} \tag{S29}$$

and, in terms of the characteristic function, for all $\mathbf{r} \in \mathbb{R}^2$ it holds that

$$\chi_{\mathscr{E}_{\lambda,\nu}(\rho)}(\mathbf{r}) = \chi_\rho(\sqrt{\lambda}\mathbf{r})e^{-\frac{1}{4}(1-\lambda)(2\nu+1)|\mathbf{r}|^2}\,. \tag{S30}$$

By exploiting (S30) and the fact that quantum states and characteristic functions are in one-to-one correspondence, for all $\lambda_1, \lambda_2 \in [0,1]$ and $\nu \geq 0$ the following composition rule holds:

$$\mathscr{E}_{\lambda_1,\nu} \circ \mathscr{E}_{\lambda_2,\nu} = \mathscr{E}_{\lambda_1\lambda_2,\nu}\,. \tag{S31}$$

In Theorem S5 we will provide a simple Kraus representation of the thermal attenuator.

1. *Bounds on two-way capacities of the thermal attenuator*

The best known upper bound on the two-way capacities of the thermal attenuator, shown by Pirandola-Laurenza-Ottaviani-Banchi (PLOB) [20], is

$$K(\mathscr{E}_{\lambda,\nu}) \leq \begin{cases} -h(\nu) - \log_2[(1-\lambda)\lambda^\nu], & \text{if } \lambda \in (\frac{\nu}{\nu+1}, 1], \\ 0, & \text{otherwise} \end{cases} \tag{S32}$$

where

$$h(\nu) := (\nu+1)\log_2(\nu+1) - \nu\log_2\nu \tag{S33}$$

is the so-called bosonic entropy. The parameter region in which such an upper bound vanishes coincides with the parameter region in which the thermal attenuator $\mathscr{E}_{\lambda,\nu}$ is entanglement breaking, i.e. $\nu \geq 0$ and $\lambda \in [0, \frac{\nu}{\nu+1}]$ [4, 21]. The best known lower bound (before our work) on $Q_2(\mathscr{E}_{\lambda,\nu})$ is given by [22]

$$Q_2(\mathscr{E}_{\lambda,\nu}) \geq \max\{0, -h(\nu) - \log_2(1-\lambda)\}\,. \tag{S34}$$

Although this is also a lower bound on $K(\mathscr{E}_{\lambda,\nu})$, it is not the best among those currently known. Indeed, an improved lower bound on $K(\mathscr{E}_{\lambda,\nu})$ has been shown by Ottaviani et al. [23]. In the energy-constrained case, the best known lower bound (before our work) on the EC two-way capacities of the thermal attenuator has been found by Noh-Pirandola-Jiang (NPJ) [24], while the best known upper bound is — depending on the parameters λ, ν, and N_s — the bound found by Davis-Shirokov-Wilde (DSW) [25] or the PLOB bound in (S32).

The lower bound in (S34) on the two-way capacities of the thermal attenuator can be proved first by applying (S20) with the choice $\rho_{AA'} = |\Psi_{N_s}\rangle\langle\Psi_{N_s}|_{AA'}$, where $|\Psi_{N_s}\rangle$ is the two-mode squeezed vacuum states with local mean photon number equal to N_s defined in (S9), second by applying the hashing inequality in (S19), and finally by proving that the reverse coherent information satisfies

$$\lim_{N_s\to\infty} I_{\mathrm{rc}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|)\right) = -h(\nu) - \log_2(1-\lambda)\,. \tag{S35}$$

Analogously, the coherent information

$$I_{\mathrm{c}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|)\right)$$

and the reverse coherent information

$$I_{\mathrm{rc}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|)\right)$$

are lower bounds on the EC two-way capacities of the thermal attenuator $\mathscr{E}_{\lambda,\nu}$ with energy constraint equal to N_s:

$$\begin{aligned} Q_2(\mathscr{E}_{\lambda,\nu}, N_s) &\geq \max\left\{I_{\mathrm{c}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|)\right), I_{\mathrm{rc}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|)\right)\right\} \\ &= \begin{cases} I_{\mathrm{c}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|)\right), & \text{if } N_s \leq \nu, \\ I_{\mathrm{rc}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|)\right), & \text{otherwise.} \end{cases} \end{aligned} \tag{S36}$$

It holds that [20, 22, 24, 26]

$$\begin{aligned} I_{\mathrm{c}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|)\right) &= h\left(\lambda N_s + (1-\lambda)\nu\right) - h\left(\frac{D + (1-\lambda)(N_s-\nu) - 1}{2}\right) - h\left(\frac{D - (1-\lambda)(N_s-\nu) - 1}{2}\right), \\ I_{\mathrm{rc}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_s}\rangle\langle\Psi_{N_s}|)\right) &= h(N_s) - h\left(\frac{D + (1-\lambda)(N_s-\nu) - 1}{2}\right) - h\left(\frac{D - (1-\lambda)(N_s-\nu) - 1}{2}\right), \end{aligned} \tag{S37}$$

where $D := \sqrt{((1+\lambda)N_s + (1-\lambda)\nu + 1)^2 - 4\lambda N_s(N_s+1)}$. The NPJ lower bound, proved by mixing forward (coherent information) and backward (reverse coherent information) strategies, is [24]

$$Q_2(\mathscr{E}_{\lambda,\nu}, N_s) \geq \sup_{\substack{x\in[0,1],\, N_1,N_2\geq 0 \\ xN_1 + (1-x)N_2 = N_s}} \left[x\, I_{\mathrm{c}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_1}\rangle\langle\Psi_{N_1}|)\right) + (1-x) I_{\mathrm{rc}}\left(\mathrm{Id}_A \otimes \mathscr{E}_{\lambda,\nu}(|\Psi_{N_2}\rangle\langle\Psi_{N_2}|)\right)\right]. \tag{S38}$$

Fixed λ and ν, if the energy constraint N_s is sufficiently large, the NPJ lower bound is equal to the reverse coherent information bound (i.e. the optimal values of the supremum problem in S38 are $x = 0$, $N_1 = 0$, and $N_2 = N_s$).

E. Thermal amplifier

Let $\mathcal{H}_S$ and $\mathcal{H}_E$ be single-mode systems and let a and b denote their annihilation operators, respectively. For all $g \geq 1$ and $\nu \geq 0$, a thermal amplifier $\Phi_{g,\nu} : \mathfrak{S}(\mathcal{H}_S) \to \mathfrak{S}(\mathcal{H}_S)$ is a quantum channel defined by

$$\Phi_{g,\nu}(\rho) := \mathrm{Tr}_E\left[U_g^{SE}(\rho^S \otimes \tau_\nu^E) U_g^{SE\dagger}\right], \tag{S39}$$

where U_g^{SE} denotes the unitary operator associated with two-mode squeezing of parameter g, i.e.

$$U_g^{SE} := \exp\left[\operatorname{arccosh}\sqrt{g}\left(a^\dagger b^\dagger - a\,b\right)\right] . \tag{S40}$$

The two-mode squeezing unitary can be expressed via the following disentangling formula [19, Appendix 5]

$$U_g^{SE} = e^{\sqrt{\frac{g-1}{g}}a^\dagger b^\dagger} e^{\frac{1}{2}\ln\left(\frac{1}{g}\right)\left(a^\dagger a - b^\dagger b + 1\right)} e^{-\sqrt{\frac{g-1}{g}}ab} . \tag{S41}$$

By writing the quadrature vector $\hat{\mathbf{R}}$ with respect the ordering (S, E), it can be shown that

$$\left(U_g^{SE}\right)^\dagger \hat{\mathbf{R}}\, U_g^{SE} = S_g\, \hat{\mathbf{R}} , \tag{S42}$$

where

$$S_g := \begin{pmatrix} \sqrt{g}\,\mathbb{1}_2 & \sqrt{g-1}\,\sigma_z \\ \sqrt{g-1}\,\sigma_z & \sqrt{g}\,\mathbb{1}_2 \end{pmatrix} . \tag{S43}$$

This implies that for all $\sigma_{SE} \in \mathfrak{S}(\mathcal{H}_S \otimes H_E)$ it holds that

$$\begin{aligned} \mathbf{m}\left(U_g^{SE}\sigma_{SE}\left(U_g^{SE}\right)^\dagger\right) &= S_g\, \mathbf{m}(\sigma_{SE}) , \\ V\left(U_g^{SE}\sigma_{SE}\left(U_g^{SE}\right)^\dagger\right) &= S_g\, V(\sigma_{SE})\, S_g^\intercal . \end{aligned} \tag{S44}$$

In terms of the annihilation operators a and b, the transformation in (S42) reads

$$\begin{aligned} \left(U_g^{SE}\right)^\dagger a\, U_g^{SE} &= \sqrt{g}\, a + \sqrt{g-1}\, b^\dagger , \\ U_g^{SE} a \left(U_g^{SE}\right)^\dagger &= \sqrt{g}\, a - \sqrt{g-1}\, b^\dagger , \\ \left(U_g^{SE}\right)^\dagger b\, U_g^{SE} &= \sqrt{g-1}\, a^\dagger + \sqrt{g}\, b , \\ U_g^{SE} b \left(U_g^{SE}\right)^\dagger &= -\sqrt{g-1}\, a^\dagger + \sqrt{g}\, b . \end{aligned} \tag{S45}$$

It can be shown that for any single-mode state ρ it holds that

$$\begin{aligned} &\mathbf{m}\left(\Phi_{g,\nu}(\rho)\right) = \sqrt{g}\,\mathbf{m}(\rho) , \\ &V\left(\Phi_{g,\nu}(\rho)\right) = g\, V(\rho) + (g-1)(2\nu+1)\mathbb{1}_2 , \end{aligned} \tag{S46}$$

and, in terms of the characteristic function, for all $\mathbf{r} \in \mathbb{R}^2$ it holds that

$$\chi_{\Phi_{g,\nu}(\rho)}(\mathbf{r}) = \chi_\rho(\sqrt{g}\mathbf{r}) e^{-\frac{1}{4}(g-1)(2\nu+1)|\mathbf{r}|^2} . \tag{S47}$$

By exploiting (S47) and the fact that quantum states and characteristic functions are in one-to-one correspondence, for all $g_1, g_2 \geq 1$ and $\nu \geq 0$ the following composition rule holds:

$$\Phi_{g_1,\nu} \circ \Phi_{g_2,\nu} = \Phi_{g_1 g_2,\nu} . \tag{S48}$$

In Theorem S5 we will provide a simple Kraus representation of the thermal amplifier.

1. *Bounds on two-way capacities of the thermal amplifier*

The best known upper bound on the two-way capacities of the thermal amplifier, shown by PLOB [20], is

$$K(\Phi_{g,\nu}) \leq \begin{cases} -h(\nu) + \log_2\left(\frac{g^{\nu+1}}{g-1}\right) , & \text{if } g \in [1, 1+\frac{1}{\nu}), \\ 0, & \text{otherwise} \end{cases} \tag{S49}$$

where $h(\nu)$ is the bosonic entropy defined in (S33). The parameter region in which such an upper bound vanishes coincides with the parameter region in which the thermal amplifier $\Phi_{g,\nu}$ is entanglement breaking, i.e. $\nu \geq 0$ and $g \geq 1 + \frac{1}{\nu}$ [4, 21]. The best known lower bound (before our work) on $Q_2(\Phi_{\lambda,\nu})$ is given by [22]

$$Q_2(\Phi_{g,\nu}) \geq \max\left\{0, -h(\nu) + \log_2\left(\frac{g}{g-1}\right)\right\} , \tag{S50}$$

which can be proved, analogously as it has been done in (S35), by showing that the coherent information satisfies

$$\lim_{N_s\to\infty} I_{\mathrm{c}}\left(\mathrm{Id}_A\otimes\Phi_{g,\nu}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|)\right) = -h(\nu)+\log_2\left(\frac{g}{g-1}\right). \tag{S51}$$

The best known lower bound on the secret-key capacity $K(\Phi_{g,\nu})$ has been shown by Wong-Ottaviani-Guo-Pirandola (WOGP) [27]. In the energy-constrained scenario, the best known lower bound is the NPJ bound [24], which is given by

$$Q_2(\Phi_{g,\nu},N_s)\geq \sup_{x\in[0,1]} x\, I_{\mathrm{c}}\left(\mathrm{Id}_A\otimes\Phi_{g,\nu}(|\Psi_{\frac{N_s}{x}}\rangle\!\langle\Psi_{\frac{N_s}{x}}|)\right), \tag{S52}$$

where [20, 22, 24, 26]

$$\begin{aligned}&I_{\mathrm{c}}\left(\mathrm{Id}_A\otimes\Phi_{g,\nu}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|)\right)\\ &= h\left(gN_s+(g-1)(\nu+1)\right)-h\left(\frac{D'+(g-1)(N_s+\nu+1)-1}{2}\right)-h\left(\frac{D'-(g-1)(N_s+\nu+1)-1}{2}\right),\end{aligned} \tag{S53}$$

with $D':=\sqrt{((g+1)N_s+(g-1)(\nu+1)+1)^2-4g\,N_s(N_s+1)}$. Fixed g and ν, if the energy constraint N_s is sufficiently large, the NPJ lower bound is equal to the coherent information bound (i.e. the optimal value of the supremum problem in S52 is $x=1$).

F. Additive Gaussian noise

Let $\mathcal{H}_S$ be a single-mode system and let $\{D_{\mathbf{r}}\}_{\mathbf{r}\in\mathbb{R}^2}$ be its dispacement operators. For all $\xi\geq 0$, the additive Gaussian noise $\Lambda_\xi:\mathfrak{S}(\mathcal{H}_S)\to\mathfrak{S}(\mathcal{H}_S)$ is a quantum channel defined by

$$\Lambda_\xi(\rho):=\frac{1}{2\pi\xi}\int_{\mathbb{R}^2}\mathrm{d}^2\mathbf{r}\,e^{-\frac{1}{2\xi}\mathbf{r}^\intercal\mathbf{r}}D_{\mathbf{r}}\rho D_{\mathbf{r}}^\dagger\,. \tag{S54}$$

By using that $\hat{\mathbf{R}}=(\hat{x},\hat{p})$, $a=\frac{\hat{x}+\hat{p}}{\sqrt{2}}$, and by defining $\mathbf{r}:=(x,p)^{\mathrm{T}}$, $z:=\frac{x+ip}{\sqrt{2}}$, and

$$D(z):=\exp\left[za^\dagger-z^*a\right]=D_{-\mathbf{r}}\,, \tag{S55}$$

the additive Gaussian noise can be expressed in the following equivalent form:

$$\Lambda_\xi(\rho)=\frac{1}{\pi\xi}\int_{\mathbb{C}}\mathrm{d}^2z\,e^{-\frac{|z|^2}{\xi}}D(z)\,\rho\,D(z)^\dagger\,, \tag{S56}$$

where we have used that $\mathrm{d}^2\mathbf{r}=\mathrm{d}x\,\mathrm{d}p=\frac{\mathrm{dRe}(z)\,\mathrm{dIm}(z)}{2}=\frac{\mathrm{d}^2z}{2}$ and we have performed the integral variable substitution $z\to -z$. It can be shown that for all single-mode states ρ it holds that

$$\begin{aligned}&\mathbf{m}\left(\Lambda_\xi(\rho)\right)=\mathbf{m}(\rho)\,,\\ &V\left(\Lambda_\xi(\rho)\right)=V(\rho)+2\xi\,\mathbb{1}_2\,.\end{aligned} \tag{S57}$$

and, in terms of the characteristic function, for all $\mathbf{r}\in\mathbb{R}^2$ it holds that

$$\chi_{\Lambda_\xi(\rho)}(\mathbf{r})=\chi_\rho(\mathbf{r})e^{-\frac{1}{2}\xi|\mathbf{r}|^2}\,. \tag{S58}$$

In Theorem S5 we will provide a simple Kraus representation of the additive Gaussian noise.

1. *Additive Gaussian noise as the strong limit of thermal attenuator or thermal amplifier*

For completeness, let us remark that the Additive Gaussian noise Λ_ξ is the strong limit of the thermal attenuator $\mathscr{E}_{1-\frac{\xi}{\nu},\nu}$ and thermal amplifier $\Phi_{1+\frac{\xi}{\nu},\nu}$ for $\nu\to\infty$, i.e. it holds that

$$\begin{aligned}&\lim_{\nu\to\infty}\|\mathscr{E}_{1-\frac{\xi}{\nu},\nu}(\rho)-\Lambda_\xi(\rho)\|_1=0\,,\\ &\lim_{\nu\to\infty}\|\Phi_{1+\frac{\xi}{\nu},\nu}(\rho)-\Lambda_\xi(\rho)\|_1=0\,,\end{aligned} \tag{S59}$$

for any single-mode state ρ. Indeed, (S30), (S47), and (S58) imply that for any single-mode state ρ and any $\mathbf{r} \in \mathbb{R}^2$ it holds that

$$\begin{aligned} \lim_{\nu\to\infty} \chi_{\mathscr{E}_{1-\frac{\xi}{\nu},\nu}(\rho)}(\mathbf{r}) &= \chi_{\Lambda_\xi(\rho)}(\mathbf{r})\,, \\ \lim_{\nu\to\infty} \chi_{\Phi_{1+\frac{\xi}{\nu},\nu}(\rho)}(\mathbf{r}) &= \chi_{\Lambda_\xi(\rho)}(\mathbf{r})\,. \end{aligned} \tag{S60}$$

Consequently, by exploiting the fact that a sequence of states $\{\sigma_k\}_{k\in\mathbb{N}} \subseteq \mathfrak{S}(L^2(\mathbb{R}))$ converges in trace norm to a quantum state $\sigma \in \mathfrak{S}(L^2(\mathbb{R}))$ if and only if the sequence of characteristic functions $\{\chi_{\sigma_k}(\mathbf{r})\}_{k\in\mathbb{N}}$ converges pointwise to the characteristic function $\chi_\sigma(\mathbf{r})$ [28, Theorem 2], the thermal attenuator $\mathscr{E}_{1-\frac{\xi}{\nu},\nu}$ and thermal amplifier $\Phi_{1+\frac{\xi}{\nu},\nu}$ strongly converge to the additive Gaussian noise Λ_ξ for $\nu \to \infty$.

2. Bounds on two-way capacities of the additive Gaussian noise

The best known upper bound on the two-way capacities of the additive Gaussian noise, shown by PLOB [20], is

$$K(\Lambda_\xi) \le \begin{cases} \frac{\xi-1}{\ln 2} - \log_2(\xi), & \text{if } \xi < 1, \\ 0, & \text{otherwise} \end{cases} \tag{S61}$$

where $h(\nu)$ is the bosonic entropy defined in (S33). The parameter region in which such an upper bound vanishes coincides with the parameter region in which the Additive Gaussian noise Λ_ξ is entanglement breaking, i.e. $\xi \ge 1$ [4, 21]. The best known lower bound (before our work) on $Q_2(\Lambda_\xi)$ is given by [22]

$$Q_2(\Lambda_\xi) \ge \max\{0, -\log_2(e\,\xi)\}\,, \tag{S62}$$

which can be proved, analogously as it has been done in (S35), by showing that the coherent information satisfies

$$\lim_{N_s\to\infty} I_{\mathrm{c}}\left(\mathrm{Id}_A \otimes \Lambda_\xi(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'})\right) = \log_2(e\,\xi)\,. \tag{S63}$$

In the energy-constrained scenario, the best known lower bound is the NPJ bound [24], which is given by

$$Q_2(\Lambda_\xi, N_s) \ge \sup_{x\in[0,1]} x\, I_{\mathrm{c}}\left(\mathrm{Id}_A \otimes \Lambda_\xi(|\Psi_{\frac{N_s}{x}}\rangle\!\langle\Psi_{\frac{N_s}{x}}|)\right)\,, \tag{S64}$$

where [20, 22, 24, 26]

$$I_{\mathrm{c}}\left(\mathrm{Id}_A \otimes \Lambda_\xi(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|)\right) = h\left(N_s+\xi\right) - h\left(\frac{D''+\xi-1}{2}\right) - h\left(\frac{D''-\xi-1}{2}\right)\,, \tag{S65}$$

with $D'' \coloneqq \sqrt{(2N_s+\xi+1)^2 - 4N_s(N_s+1)}$. Fixed ξ, if the energy constraint N_s is sufficiently large, the NPJ lower bound is equal to the coherent information bound (i.e. the optimal value of the supremum problem in S64 is $x = 1$).

II. ACTION OF PHASE-INSENSITIVE BOSONIC GAUSSIAN CHANNELS ON GENERIC OPERATORS

In this section we establish properties of the channel composition between pure amplifier channel and pure loss channel.

Definition 1. For all $\lambda \in [0,1]$ and $g \ge 1$ let us define the channel $\mathscr{N}_{g,\lambda}$ as the composition between pure amplifier channel $\Phi_{g,0}$ and pure loss channel $\mathscr{E}_{\lambda,0}$, i.e.

$$\mathscr{N}_{g,\lambda} \coloneqq \Phi_{g,0} \circ \mathscr{E}_{\lambda,0}\,. \tag{S66}$$

Lemma S3. *The channel $\mathscr{N}_{g,\lambda}$ is entanglement breaking if and only if $(1-\lambda)g \ge 1$.*

Proof. First, let us determine the parameter region of g and λ where the channel $\mathcal{N}_{g,\lambda}$ is entanglement breaking. Since $\mathcal{N}_{g,\lambda}$ is a Gaussian channel, we can apply Lemma S2. By using (S72), one can show that $\mathcal{N}_{g,\lambda}$ transforms the first moment and the covariance matrix as

$$\begin{aligned} \mathbf{m}\left(\mathcal{N}_{g,\lambda}(\rho)\right) &= \sqrt{g\lambda}\,\mathbf{m}(\rho)\,, \\ V\left(\mathcal{N}_{g,\lambda}(\rho)\right) &= g\lambda\, V(\rho) + (2g-1-g\lambda)\,\mathbb{1}_2\,, \end{aligned} \tag{S67}$$

for all quantum states ρ. Hence, Lemma S2 establishes that Φ is entanglement breaking if and only if there exists $\alpha, \gamma \in \mathbb{R}^{2\times 2}$ with $\alpha \geq i\,\Omega_1$ and $\gamma \geq i\lambda g\,\Omega_1$ such that

$$(2g-1-g\lambda)\,\mathbb{1}_2 = \alpha + \gamma\,. \tag{S68}$$

The condition in (S68) is equivalent to

$$(2g-1-g\lambda)\,\mathbb{1}_2 \geq i\,(1+\lambda g)\,\Omega_1\,. \tag{S69}$$

Indeed, if the condition in (S68) is satisfied, then $(2g-1-g\lambda)\,\mathbb{1}_2 = \alpha+\gamma \geq i\,(1+\lambda g)\,\Omega_1$, i.e. also the condition in (S69) is satisfied. Conversely, assume that the condition in (S69) is satisfied. Then, the fact that

$$x\,\mathbb{1}_2 \geq i\,\Omega_1 \quad \text{if and only if} \quad x \geq 1\,, \tag{S70}$$

implies that $(1-\lambda)g \geq 1$. Consequently, by choosing $\alpha := \mathbb{1}_2$ and $\gamma := (2g-2-g\lambda)\mathbb{1}_2$ and by using (S70), it holds that the condition in (S68) is satisfied with $\alpha \geq i\,\Omega_1$ and $\gamma \geq i\lambda g\,\Omega_1$. By exploiting (S70), we deduce that $\mathcal{N}_{g,\lambda}$ is entanglement breaking if and only if $(1-\lambda)g \geq 1$. ☐

Lemma S4. *Let $\nu \geq 0$, $\lambda \in [0,1]$, $g \geq 1$, and $\xi \geq 0$. The thermal attenuator $\mathcal{E}_{\lambda,\nu}$, the thermal amplifier $\Phi_{g,\nu}$, and the additive Gaussian noise Λ_ξ can be expressed in terms of the composition between pure amplifier channel and pure loss channel as*

$$\begin{aligned} \mathcal{E}_{\lambda,\nu} &= \mathcal{N}_{1+(1-\lambda)\nu\,,\,\frac{\lambda}{1+(1-\lambda)\nu}}\,, \\ \Phi_{g,\nu} &= \mathcal{N}_{g+(g-1)\nu\,,\,\frac{g}{g+(g-1)\nu}}\,, \\ \Lambda_\xi &= \mathcal{N}_{1+\xi\,,\,\frac{1}{1+\xi}}\,. \end{aligned} \tag{S71}$$

Proof. Let ρ be a single-mode state. The characteristic function of $\mathcal{N}_{g,\lambda}(\rho)$ is

$$\chi_{\mathcal{N}_{g,\lambda}(\rho)}(\mathbf{r}) = \chi_{\Phi_{g,0}\circ\mathcal{E}_{\lambda,0}(\rho)}(\mathbf{r}) = \chi_{\mathcal{E}_{\lambda,0}(\rho)}(\sqrt{g}\mathbf{r})e^{-\frac{1}{4}(g-1)|\mathbf{r}|^2} = \chi_\rho(\sqrt{g\lambda}\,\mathbf{r})e^{-\frac{1}{4}[2g-1-g\lambda]|\mathbf{r}|^2} \tag{S72}$$

for all $\mathbf{r} \in \mathbb{R}^2$, where we have used (S30) and (S47). Consequently, by exploiting (S30), (S47), and (S58), one can check that for all $\mathbf{r} \in \mathbb{R}^2$ it holds that

$$\begin{aligned} \chi_{\mathcal{E}_{\lambda,\nu}(\rho)}(\mathbf{r}) &= \chi_{\mathcal{N}_{1+(1-\lambda)\nu\,,\,\frac{\lambda}{1+(1-\lambda)\nu}}(\rho)}(\mathbf{r})\,, \\ \chi_{\Phi_{g,\nu}(\rho)}(\mathbf{r}) &= \chi_{\mathcal{N}_{g+(g-1)\nu\,,\,\frac{g}{g+(g-1)\nu}}(\rho)}(\mathbf{r})\,, \\ \chi_{\Lambda_\xi(\rho)}(\mathbf{r}) &= \chi_{\mathcal{N}_{1+\xi\,,\,\frac{1}{1+\xi}}(\rho)}(\mathbf{r})\,. \end{aligned} \tag{S73}$$

Hence, by exploiting the fact that quantum states and characteristic functions are in one-to-one correspondence, (S71) is proved. ☐

The forthcoming Theorem S5 provides a simple Kraus representation of $\mathcal{N}_{g,\lambda}$ and allows one to easily calculate the output of $\mathcal{N}_{g,\lambda}$ for generic input operators.

Theorem S5. *Let $\lambda \in [0,1]$ and $g \geq 1$. The quantum channel $\mathcal{N}_{g,\lambda}$, defined in Definition (1), admits the following Kraus representation:*

$$\mathcal{N}_{g,\lambda}(\rho) = \sum_{k,m=0}^{\infty} M_{k,m}^{(comp)}(g,\lambda)\,\rho\left(M_{k,m}^{(comp)}(g,\lambda)\right)^\dagger\,, \tag{S74}$$

where

$$M_{k,m}^{(comp)}(g,\lambda) := M_k^{(pure\ amp)}(g)\,M_m^{(pure\ loss)}(\lambda) = \sqrt{\frac{(g-1)^k\,(1-\lambda)^m}{k!\,m!\,g^{k+1}}}(a^\dagger)^k\left(\sqrt{\frac{\lambda}{g}}\right)^{a^\dagger a} a^m \tag{S75}$$

and where we have introduced the Kraus operators of pure loss channel and pure amplifier channel:

$$M_k^{(pure\ amp)}(g) := \frac{1}{\sqrt{g\,k!}}\left(\sqrt{\frac{g-1}{g}}\right)^k (a^\dagger)^k \left(\frac{1}{\sqrt{g}}\right)^{a^\dagger a}\,, \tag{S76}$$

$$M_m^{(pure\ loss)}(\lambda) := \sqrt{\frac{(1-\lambda)^m}{m!}}(\sqrt{\lambda})^{a^\dagger a}\, a^m\,. \tag{S77}$$

In particular, by letting $|n\rangle$ and $|i\rangle$ two Fock states, it holds that

$$\mathscr{N}_{g,\lambda}(|n\rangle\langle i|) = \sum_{l=\max(i-n,0)}^{\infty} f_{n,i,l}(g,\lambda)\,|l+n-i\rangle\langle l|\,. \tag{S78}$$

where

$$f_{n,i,l}(g,\lambda) := \sum_{m=\max(i-l,0)}^{\min(n,i)} \frac{\sqrt{n!i!l!(l+n-i)!}}{(n-m)!(i-m)!m!(l+m-i)!}\,\frac{(g-1)^{l+m-i}(1-\lambda)^m\lambda^{\frac{n+i-2m}{2}}}{g^{l+1+\frac{n-i}{2}}}\,. \tag{S79}$$

Proof. By using (S22), the pure loss channel can be written as

$$\mathscr{E}_{\lambda,0}(\rho) = \sum_{m=0}^{\infty} M_m^{(\text{pure loss})}(\lambda)\,\rho\left(M_m^{(\text{pure loss})}(\lambda)\right)^\dagger\,, \tag{S80}$$

where for all $m \in \mathbb{N}$ the Kraus operator $M_m^{(\text{pure loss})}(\lambda)$ is

$$M_m^{(\text{pure loss})}(\lambda) := (-1)^m \langle m|_E\, U_\lambda^{SE}\, |0\rangle_E\,. \tag{S81}$$

Hence, by using the disentangling formula for beam splitter unitary [19, Appendix 5]

$$U_\lambda^{SE} = e^{-\sqrt{\frac{1-\lambda}{\lambda}}ab^\dagger} e^{\frac{1}{2}\ln\lambda\left(a^\dagger a - b^\dagger b\right)} e^{\sqrt{\frac{1-\lambda}{\lambda}}a^\dagger b} \tag{S82}$$

and the fact that

$$e^{-\frac{1}{2}\ln\lambda\, a^\dagger a}\, a^m\, e^{\frac{1}{2}\ln\lambda\, a^\dagger a} = \lambda^{m/2} a\,, \tag{S83}$$

it holds that

$$M_m^{(\text{pure loss})}(\lambda) = \frac{1}{\sqrt{m!}}\left(\sqrt{\frac{1-\lambda}{\lambda}}\right)^m a^m e^{\frac{1}{2}\ln\lambda\, a^\dagger a} = \sqrt{\frac{(1-\lambda)^m}{m!}}(\sqrt{\lambda})^{a^\dagger a}\, a^m\,. \tag{S84}$$

By using (S39), the pure amplifier channel can be written as

$$\Phi_{g,0}(\rho) = \sum_{k=0}^{\infty} M_k^{(\text{pure amp})}(g)\,\rho\left(M_k^{(\text{pure amp})}(g)\right)^\dagger\,, \tag{S85}$$

where for all $k \in \mathbb{N}$ the Kraus operator $M_k^{(\text{pure amp})}(g)$ is

$$M_k^{(\text{pure amp})}(g) := \langle k|_E\, U_g^{SE}\, |0\rangle_E\,. \tag{S86}$$

Hence, by using the disentangling formula for the two-mode squeezing unitary [19, Appendix 5]

$$U_g^{SE} = e^{\sqrt{\frac{g-1}{g}}a^\dagger b^\dagger} e^{\frac{1}{2}\ln\left(\frac{1}{g}\right)\left(a^\dagger a - b^\dagger b + 1\right)} e^{-\sqrt{\frac{g-1}{g}}ab}\,, \tag{S87}$$

it holds that

$$M_k^{(\text{pure amp})}(g) = \frac{1}{\sqrt{g\,k!}}\left(\sqrt{\frac{g-1}{g}}\right)^k (a^\dagger)^k \left(\frac{1}{\sqrt{g}}\right)^{a^\dagger a}\,. \tag{S88}$$

By using (S80), (S85), and the fact $\mathcal{N}_{g,\lambda} = \Phi_{g,0} \circ \mathcal{E}_{\lambda,0}$, (S74) is proved. Now, let us calculate $\mathcal{N}_{g,\lambda}(|n\rangle\langle i|) = \sum_{m,n=0}^{\infty} M_{k,m}^{(\mathrm{comp})}(g,\lambda)\,|n\rangle\langle i|\,(M_{k,m}^{(\mathrm{comp})}(g,\lambda))^\dagger$ in order to prove (S78). By exploiting the following formulae

$$\begin{aligned} a^m\,|n\rangle &= \begin{cases} \sqrt{\frac{n!}{(n-m)!}}\,|n-m\rangle\,, & \text{if } n \geq m, \\ 0, & \text{otherwise} \end{cases} \\ \left(a^\dagger\right)^k |n-m\rangle &= \sqrt{\frac{(n-m+k)!}{(n-m)!}}\,|n-m+k\rangle\,, \end{aligned} \tag{S89}$$

for $m > n$ it holds that $M_{k,m}\,|n\rangle = 0$, otherwise for $m \leq n$ it holds that

$$M_{k,m}^{(comp)}(g,\lambda)\,|n\rangle = \frac{1}{(n-m)!}\sqrt{\frac{n!(n-m+k)!}{k!m!}}\sqrt{\frac{(g-1)^k(1-\lambda)^m\lambda^{n-m}}{g^{k+1+n-m}}}\,|n-m+k\rangle\,. \tag{S90}$$

Consequently, we conclude that

$$\begin{aligned} \mathcal{N}_{g,\lambda}(|n\rangle\langle i|) &= \sum_{k=0}^{\infty}\sum_{m=0}^{\min(n,i)} \frac{\sqrt{n!(n-m+k)!i!(i-m+k)!}}{(n-m)!(i-m)!k!m!}\sqrt{\frac{(g-1)^{2k}(1-\lambda)^{2m}\lambda^{n+i-2m}}{g^{2k+2+n+i-2m}}}\,|n-m+k\rangle\langle i-m+k| \\ &= \sum_{l=\max(i-n,0)}^{\infty} f_{n,i,l}(g,\lambda)\,|l+n-i\rangle\langle l|\,. \end{aligned} \tag{S91}$$

Hence, (S78) is proved. □

Calculating the action of Gaussian channels on non-Gaussian states is cumbersome in general. The forthcoming Theorem S6 overcomes this difficulty and allows one to easily calculate the output of all piBGCs for generic input operators.

Theorem S6. *Let $\nu \geq 0$, $\lambda \in [0,1]$, $g \geq 1$, and $\xi \geq 0$. The thermal attenuator $\mathcal{E}_{\lambda,\nu}$, the thermal amplifier $\Phi_{g,\nu}$, and the additive Gaussian noise Λ_ξ admit the following Kraus representations:*

$$\mathcal{E}_{\lambda,\nu}(\rho) = \sum_{k,m=0}^{\infty} M_{k,m}^{(att)}(\lambda,\nu)\,\rho\left(M_{k,m}^{(att)}(\lambda,\nu)\right)^\dagger\,, \tag{S92}$$

$$\Phi_{g,\nu}(\rho) = \sum_{k,m=0}^{\infty} M_{k,m}^{(amp)}(g,\nu)\,\rho\left(M_{k,m}^{(amp)}(g,\nu)\right)^\dagger\,, \tag{S93}$$

$$\Lambda_\xi(\rho) = \sum_{k,m=0}^{\infty} M_{k,m}^{(add)}(\xi)\,\rho\left(M_{k,m}^{(add)}(\xi)\right)^\dagger\,, \tag{S94}$$

where

$$M_{k,m}^{(att)}(\lambda,\nu) := M_{k,m}^{(comp)}\left(1+(1-\lambda)\nu, \frac{\lambda}{1+(1-\lambda)\nu}\right)\,, \tag{S95}$$

$$M_{k,m}^{(amp)}(g,\nu) := M_{k,m}^{(comp)}\left(g+(g-1)\nu, \frac{g}{g+(g-1)\nu}\right)\,, \tag{S96}$$

$$M_{k,m}^{(add)}(\xi) := M_{k,m}^{(comp)}\left(1+\xi, \frac{1}{1+\xi}\right)\,, \tag{S97}$$

with $M_{k,m}^{(comp)}$ being defined in (S75). *In particular, by letting $|n\rangle$ and $|i\rangle$ two Fock states, it holds that*

$$\mathcal{E}_{\lambda,\nu}(|n\rangle\langle i|) = \sum_{l=\max(i-n,0)}^{\infty} f_{n,i,l}\left(1+(1-\lambda)\nu, \frac{\lambda}{1+(1-\lambda)\nu}\right)\,|l+n-i\rangle\langle l|\,, \tag{S98}$$

$$\Phi_{g,\nu}(|n\rangle\!\langle i|) = \sum_{l=\max(i-n,0)}^{\infty} f_{n,i,l}\left(g+(g-1)\nu, \frac{g}{g+(g-1)\nu}\right) |l+n-i\rangle\!\langle l| \,, \tag{S99}$$

$$\Lambda_{\xi}(|n\rangle\!\langle i|) = \sum_{l=\max(i-n,0)}^{\infty} f_{n,i,l}\left(1+\xi, \frac{1}{1+\xi}\right) |l+n-i\rangle\!\langle l| \,, \tag{S100}$$

with $f_{n,i,l}$ *being defined in* (S79).

Proof. Theorem S6 is a direct consequence of Lemma S4 and Theorem S5. □

We observe here that the Kraus representation in (S95) of the thermal attenuator is precisely the one obtained in [29] via the "master equation trick".

III. RESULTS

In this section we expound our results. In subsection III A first we prove preliminary results on the two-way capacities of generic quantum channels and second we apply them to the composition between pure amplifier channel and pure loss channel. In subsection V we specialise these results to the case of piBGCs (thermal attenuator, thermal amplifier, and additive Gaussian noise) and we find the following two main results:

- The parameter regions where the (EC) two-way capacities of piBGCs are strictly positive are precisely those where these channels are not entanglement breaking;
- We find a new lower bound on the secret-key and two-way quantum capacity of piBGCs, which constitutes a significant improvement with respect the state-of-the-art lower bounds [22–24, 27, 30] in many parameter regions.

A. Preliminary results

Let us begin by introducing the concept of a *generalized Choi state* of a quantum channel.

Definition S7 Generalised Choi state of a quantum channel [31, 32]**.** *Let* $\mathcal{H}_B$ *be a possibly infinite-dimensional Hilbert space. Let* $\mathcal{H}_A, \mathcal{H}_{A'}$ *be isomorphic (possibly infinite dimensional) Hilbert spaces. Let* $|\psi\rangle_{A'A}$ *be a pure state of the form*

$$|\psi\rangle_{A'A} = \sum_i \sqrt{\lambda_i}\, |e_i\rangle_A \otimes |e_i\rangle_{A'} \,, \tag{S101}$$

where $(\lambda_i)_i$ *are strictly positive numbers such that* $\sum_i \lambda_i = 1$*, and* $(|e_i\rangle_A)_i$ *and* $(|e_i\rangle_{A'})_i$ *form an orthonormal basis of* $\mathcal{H}_A$ *and* $\mathcal{H}_{A'}$*, respectively. Let* $\Phi_{A'\to B}$ *be a quantum channel from* $\mathcal{H}_{A'}$ *to* $\mathcal{H}_B$*. Then, the state*

$$C_{AB} \coloneqq \mathrm{Id}_A \otimes \Phi_{A'\to B}(|\psi\rangle\!\langle\psi|_{AA'}) \tag{S102}$$

is said to be a generalised Choi state of Φ*.*

In finite dimensions, if the state $|\psi\rangle$ in (S101) is a *maximally entangled state*, then the state $C_{AB} \coloneqq \mathrm{Id}_A \otimes \Phi_{A'\to B}(|\psi\rangle\!\langle\psi|_{AA'})$ is simply referred to as the Choi state of the channel Φ. Additionally, it is well known that a quantum channel is completely characterised by its Choi state [5]. The following lemma extends this result, showing that a quantum channel can also be completely characterised in terms of its *generalised* Choi state.

Lemma S8. *Let* $\Phi_{A'\to B}$ *be a quantum channel and let be* C_{AB} *a generalised Choi state. Then, it holds that*

$$\Phi_{A'\to B}(X_{A'}) = \mathrm{Tr}_A\!\left[(X_A \otimes \mathbb{1}_B)\,(D_A \otimes \mathbb{1}_B)\, C_{AB}^{t_A}\,(D_A \otimes \mathbb{1}_B)\right] \quad \textit{for all linear operators } X_{A'} \,, \tag{S103}$$

where, by using the notation introduced in Definition S7, $D_A \coloneqq \sum_i \lambda_i^{-1/2}\, |e_i\rangle\!\langle e_i|_A$ *and* t_A *is the partial transpose on* A*, i.e.* $(|e_i\rangle\!\langle e_j|_A)^{t_A} = |e_j\rangle\!\langle e_i|_A$ *for all* i, j*.*

Proof. By exploiting that $(|e_i\rangle_A)_i$ are orthonormal, we have that

$$\Phi_{A'\to B}\big(|e_i\rangle\!\langle e_j|_{A'}\big) = \frac{1}{\sqrt{\lambda_i\lambda_j}}\,\mathrm{Tr}_A[(|e_j\rangle\!\langle e_i|_A \otimes \mathbb{1}_B)\ C_{AB}]\,, \quad \forall\, i,j\,. \tag{S104}$$

By writing

$$X_{A'} = \sum_{ij} \langle e_i|\, X\, |e_j\rangle\, |e_i\rangle\!\langle e_j|_{A'} \tag{S105}$$

and by exploiting the linearity of $\Phi_{A'\to B}$, it thus follows that

$$\begin{aligned}
\Phi_{A'\to B}(X_{A'}) &= \mathrm{Tr}_A\big[\big((D_A X_A D_A)^{t_A} \otimes \mathbb{1}_B\big)\ C_{AB}\big] \\
&= \mathrm{Tr}_A\big[(D_A X_A D_A \otimes \mathbb{1}_B)\ C_{AB}^{t_A}\big] \\
&= \mathrm{Tr}_A\big[(X_A \otimes \mathbb{1}_B)\ (D_A \otimes \mathbb{1}_B)\, C_{AB}^{t_A}\, (D_A \otimes \mathbb{1}_B)\big]\ .
\end{aligned} \tag{S106}$$

□

In finite dimensions, it is well known that a quantum channel is entanglement breaking if and only if its Choi state is separable. The following lemma generalises this result, demonstrating that a quantum channel is entanglement breaking if and only if its *generalised* Choi state is separable.

Lemma S9. *Let Φ be a quantum channel and let C_{AB} be a generalised Choi state of Φ. Then, Φ is entanglement breaking if and only if C_{AB} is separable.*

Proof. By definition, if Φ is entanglement breaking, then $\mathrm{Id}_R \otimes \Phi_{A'\to B}(\rho_{RA'})$ is separable for all bipartite states $\rho_{RA'}$. In particular, any generalised Choi state of an entanglement breaking channel is separable.

Conversely, let us assume that the generalised Choi state C_{AB} is separable, that is there exists a probability distribution p_x and states $(\rho_A^{(x)})_x, (\sigma_B^{(x)})_x$ such that

$$C_{AB} = \sum_x p_x\, \rho_A^{(x)} \otimes \sigma_B^{(x)}\,. \tag{S107}$$

Let us show that Φ is entanglement breaking. To this end let us consider an arbitrary bipartite state $\rho_{RA'}$ and let us show that $\mathrm{Id}_R \otimes \Phi_{A'\to B}(\rho_{RA'})$ is separable. By exploiting Lemma S8, it holds that

$$\begin{aligned}
\mathrm{Id}_R \otimes \Phi_{A'\to B}(\rho_{RA'}) &= \mathrm{Tr}_A\big[(\rho_{RA} \otimes \mathbb{1}_B)\ \big(\mathbb{1}_R \otimes (D_A \otimes \mathbb{1}_B)\, C_{AB}^{t_A}\, (D_A \otimes \mathbb{1}_B)\big)\big] \\
&= \sum_x p_x\ \mathrm{Tr}_A\Big[\rho_{RA}\ \Big(\mathbb{1}_R \otimes D_A\, (\rho_A^{(x)})^{t_A}\, D_A\Big)\Big] \otimes \sigma_B^{(x)}\,.
\end{aligned} \tag{S108}$$

Since the operator $D_A\, (\rho_A^{(x)})^{t_A}\, D_A$ is positive semidefinite, we can write its spectral decomposition as

$$D_A\, (\rho_A^{(x)})^{t_A}\, D_A = \sum_i \eta_i^{(x)}\, |\phi_i^{(x)}\rangle\!\langle \phi_i^{(x)}| \tag{S109}$$

with the eigenvalues $(\eta_i^{(x)})_i$ being positive. This implies that the operator $\mathrm{Tr}_A\Big[\rho_{RA}\ \Big(\mathbb{1}_R \otimes D_A\, (\rho_A^{(x)})^{t_A}\, D_A\Big)\Big]$ is positive semidefinite, as it can be written as

$$\mathrm{Tr}_A\Big[\rho_{RA}\ \Big(\mathbb{1}_R \otimes D_A\, (\rho_A^{(x)})^{t_A}\, D_A\Big)\Big] = \sum_i \eta_i^{(x)}\, \langle \phi_i^{(x)}|_A\, \rho_{RA}\, |\phi_i^{(x)}\rangle_A\ . \tag{S110}$$

and $\langle \phi_i^{(x)}|_A\, \rho_{RA}\, |\phi_i^{(x)}\rangle_A$ is positive semidefinite. In particular, the trace of the operator $\mathrm{Tr}_A\Big[\rho_{RA}\ \Big(\mathbb{1}_R \otimes D_A\, (\rho_A^{(x)})^{t_A}\, D_A\Big)\Big]$ vanishes if and only if it is the zero operator. Consequently, (S108) implies that

$$\mathrm{Id}_R \otimes \Phi_{A'\to B}(\rho_{RA'}) = \sum_{x:\, q_x \neq 0} q_x\, \omega_R^{(x)} \otimes \sigma_B^{(x)}\,, \tag{S111}$$

where we defined

$$q_x := p_x \operatorname{Tr}_{RA}\Big[\rho_{RA}\ \Big(\mathbb{1}_R \otimes D_A\,(\rho_A^{(x)})^{t_A}\,D_A\Big)\Big]\ ,$$
$$\omega_R^{(x)} := \frac{\operatorname{Tr}_A\Big[\rho_{RA}\ \Big(\mathbb{1}_R \otimes D_A\,(\rho_A^{(x)})^{t_A}\,D_A\Big)\Big]}{\operatorname{Tr}_{RA}\Big[\rho_{RA}\ \Big(\mathbb{1}_R \otimes D_A\,(\rho_A^{(x)})^{t_A}\,D_A\Big)\Big]}\,. \tag{S112}$$

The fact that the operator $\operatorname{Tr}_A\Big[\rho_{RA}\ \Big(\mathbb{1}_R \otimes D_A\,(\rho_A^{(x)})^{t_A}\,D_A\Big)\Big]$ is positive semidefinite implies that $(q_x)_x$ is a probability distribution and that $\omega_R^{(x)}$ is a quantum state. Hence, we conclude that $\mathrm{Id}_R \otimes \Phi_{A'\to B}(\rho_{RA'})$ is separable. □

The following theorem establishes that the energy-constrained two-way capacities of a single-mode Gaussian channel are strictly positive if and only if the channel is not entanglement breaking.

Theorem S10. *Let Φ be a single-mode Gaussian channel and let $N_s > 0$. The energy-constrained two-way quantum capacity $Q_2(\Phi, N_s)$ and secret-key capacity $K(\Phi, N_s)$ are strictly positive if and only if Φ is not entanglement breaking.*

Proof. Since any entanglement-breaking channel has vanishing two-way capacities [5], it suffices to consider the case where Φ is not entanglement breaking. Assume that Alice prepares many copies of the two-mode squeezed vacuum state $|\Psi_{N_s}\rangle_{AA'}$ with mean local photon number N_s and sends the systems A' through the Gaussian channel $\Phi_{A'\to B}$. Now Alice and Bob share many copies of the two-mode Gaussian state $C_{N_s} := \big(\mathrm{Id}_A \otimes \Phi_{A'\to B}\big)(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'})$, which is a generalised Choi state of Φ [1, 31]. As such, C_{N_s} is entangled, as established by Lemma S9. By exploiting the fact that a two-mode Gaussian state is entangled if and only if it is not PPT [1, 2, 33], it thus follows that C_{N_s} is not PPT. Since any two-mode Gaussian state that it is not PPT is also *distillable* [34] — i.e. it can be converted into ebits with a strictly positive rate — we conclude that $K(\Phi, N_s) \geq Q_2(\Phi, N_s) > 0$. □

In the following, we provide an alternative, more explicit proof of the above result. We start by proving the following lemma.

Lemma S11. *Let $\Phi : \mathfrak{S}(L^2(\mathbb{R})) \to \mathfrak{S}(L^2(\mathbb{R}))$ be a single-mode Gaussian quantum channel and let $N_s > 0$. Suppose that $f\,(\mathrm{Id} \otimes \Phi(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|)) < 0$, where $|\Psi_{N_s}\rangle$ is the two-mode squeezed vacuum state defined in* (S9) *and f is the function defined in Lemma S1. The energy-constrained two-way capacities $Q_2(\Phi, N_s)$ and $K(\Phi, N_s)$ are strictly positive. In particular, the (unconstrained) two-way capacities $Q_2(\Phi)$ and $K(\Phi)$ are strictly positive.*

Proof. Since the state $\mathrm{Id} \otimes \Phi(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|)$ is a two-mode Gaussian state, we can apply Lemma S1 to conclude that it is entangled. Consequently, since any two-mode Gaussian entangled state is distillable [34], then $\mathrm{Id} \otimes \Phi(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|)$ is distillable. Hence, by exploiting (S20), we deduce that $Q_2(\Phi, N_s) > 0$. In addition, (S16) implies that $K(\Phi, N_s) > 0$. Finally, since the energy-constrained capacities are lower bounds on the corresponding unconstrained capacities, we conclude that the unconstrained two-way capacities of Φ are strictly positive. □

The forthcoming Theorem S12 determines the parameter region of $g \geq 1$ and $\lambda \in [0, 1]$ where the composition $\mathscr{N}_{g,\lambda} := \Phi_{g,0} \circ \mathscr{E}_{\lambda,0}$ between pure amplifier channel $\Phi_{g,0}$ and pure loss channel $\mathscr{E}_{\lambda,0}$ has strictly positive (EC) two-way capacities. In particular, we show that the (EC) two-way capacities of $\mathscr{N}_{g,\lambda}$ are strictly positive if and only if $\mathscr{N}_{g,\lambda}$ is not entanglement breaking.

Theorem S12. *Let $\lambda \in [0, 1]$, $g \geq 1$, and $N_s > 0$. The energy-constrained two-way capacities $Q_2(\mathscr{N}_{g,\lambda}, N_s)$ and $K(\mathscr{N}_{g,\lambda}, N_s)$ are strictly positive if and only if $(1-\lambda)g < 1$, i.e. if and only if $\mathscr{N}_{g,\lambda}$ is not entanglement breaking. In particular, the same holds for the unconstrained two-way capacities.*

Proof. Suppose that $(1-\lambda)g \geq 1$. Then Lemma S3 implies that $\mathscr{N}_{g,\lambda}$ is entanglement breaking and hence [35] its two way-capacities vanish.

Now, suppose that $(1-\lambda)g < 1$. Let us check that the hypothesis of Lemma S11 is fulfilled, i.e. we need to check that $f\,(\mathrm{Id} \otimes \mathscr{N}_{g,\lambda}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|)) < 0$, where $|\Psi_{N_s}\rangle$ is the two-mode squeezed vacuum state defined in (S9) and f is the function defined in Lemma S1. Let us calculate the covariance matrix of the state

$$\begin{aligned}&\mathrm{Id}_A \otimes \mathscr{N}_{g,\lambda}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'})\\ &= \operatorname{Tr}_{E_1E_2}\Big[\Big(\mathbb{1}_A \otimes U_g^{A'E_1} \otimes U_\lambda^{A'E_2}\Big)\ |\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'} \otimes |0\rangle\!\langle 0|_{E_1} \otimes |0\rangle\!\langle 0|_{E_2}\ \Big(\mathbb{1}_A \otimes U_g^{A'E_1} \otimes U_\lambda^{A'E_2}\Big)^\dagger\Big]\end{aligned} \tag{S113}$$

with respect the ordering (A, A', E_1, E_2). By using (S27) and (S44), one can show that the covariance matrix of

$$\Big(\mathbb{1}_A \otimes U_g^{A'E_1} \otimes U_\lambda^{A'E_2}\Big)\ |\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'} \otimes |0\rangle\!\langle 0|_{E_1} \otimes |0\rangle\!\langle 0|_{E_2}\ \Big(\mathbb{1}_A \otimes U_g^{A'E_1} \otimes U_\lambda^{A'E_2}\Big)^\dagger \tag{S114}$$

with respect the ordering (A, A', E_1, E_2) is

$$(\mathbb{1}_2 \oplus S_g \oplus \mathbb{1}_2)\left(\mathbb{1}_2 \oplus \bar{S}_\lambda\right)\left(V(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'}) \oplus V(|0\rangle\!\langle 0|) \oplus V(|0\rangle\!\langle 0|)\right)\left(\mathbb{1}_2 \oplus \bar{S}_\lambda^\intercal\right)\left(\mathbb{1}_2 \oplus S_g^\intercal \oplus \mathbb{1}_2\right), \tag{S115}$$

where

$$\bar{S}_\lambda := \begin{pmatrix} \sqrt{\lambda}\,\mathbb{1}_2 & 0_{2\times 2} & \sqrt{1-\lambda}\,\mathbb{1}_2 \\ 0_{2\times 2} & \mathbb{1}_2 & 0_{2\times 2} \\ -\sqrt{1-\lambda}\,\mathbb{1}_2 & 0_{2\times 2} & \sqrt{\lambda}\,\mathbb{1}_2 \end{pmatrix} \tag{S116}$$

and $0_{2\times 2} := \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Hence, since $V\left(\mathrm{Id}_A \otimes \mathcal{N}_{g,\lambda}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'})\right)$ is the 4×4 upper-left block of the covariance matrix in (S115), one can show that

$$V\left(\mathrm{Id}_A \otimes \mathcal{N}_{g,\lambda}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'})\right) = \begin{pmatrix} (2N_s+1)\mathbb{1}_2 & 2\sqrt{g\lambda N_s(N_s+1)}\sigma_z \\ 2\sqrt{g\lambda N_s(N_s+1)}\sigma_z & [2g\,(1+\lambda N_s)-1]\mathbb{1}_2 \end{pmatrix}, \tag{S117}$$

where we used (S8) and (S11). Consequently, since

$$f\left(\mathrm{Id}_A \otimes \mathcal{N}_{g,\lambda}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'}\right) = -16N_s(1+N_s)g\,(1-(1-\lambda)g)\,, \tag{S118}$$

and since $(1-\lambda)g < 1$, we have that $f\left(\mathrm{Id}_A \otimes \mathcal{N}_{g,\lambda}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'}\right) < 0$, i.e. the hypothesis of Lemma S11 is fulfilled. Hence, Lemma S11 implies that the energy-constrained two-way capacities of $\mathcal{N}_{g,\lambda}$ are strictly positive. This concludes the proof of Theorem S12. In Remark 1 we will provide an alternative proof. □

In the forthcoming Theorem S13 we obtain a lower bound on the two-way capacities of a quantum channel $\Phi : \mathfrak{S}(L^2(\mathbb{R})) \to \mathfrak{S}(L^2(\mathbb{R}))$ by introducing a protocol to distribute ebits though Φ. The idea of such a protocol is the following. First, Alice prepares states of the form

$$|\Psi_{M,c}\rangle_{AA'} := c\,|0\rangle_A\,|0\rangle_{A'} + \sqrt{1-c^2}\,|M\rangle_A\,|M\rangle_{A'}\,, \tag{S119}$$

where $M \in \mathbb{N}^+$ and $c \in (0,1)$. Then, she sends the halves A' to Bob trough Φ, who makes a measurement on each half in order to project his half onto the span of $\{|0\rangle, |M\rangle\}$. Then, Alice and Bob run k times the P1-or-P2 recurrence protocol [16] on the resulting states. After this, Alice and Bob run the improved hashing protocol introduced in [17] in order to generate ebits. Let $R(\Phi, M, c, k)$ be the rate of distributed ebits of this protocol. A lower bound on $Q_2(\Phi)$ (and hence on $K(\Phi)$) can be obtained by maximising $R(\Phi, M, c, k)$ over $M \in \mathbb{N}^+$, $c \in (0,1)$, and $k \in \mathbb{N}$.

Theorem S13. *Let $\Phi : \mathfrak{S}(L^2(\mathbb{R})) \to \mathfrak{S}(L^2(\mathbb{R}))$ be a quantum channel which maps a single-mode system A' into another single-mode system B. The EC two-way capacities $Q_2(\Phi, N_s)$ and $K(\Phi, N_s)$ satisfy the following lower bound*

$$K(\Phi, N_s) \ge Q_2(\Phi, N_s) \ge \sup_{\substack{c\in(0,1),\, M\in\mathbb{N}^+,\, k\in\mathbb{N} \\ (1-c^2)M \le N_s}} R(\Phi, M, c, k)\,, \tag{S120}$$

and, in particular, the unconstrained two-way capacities satisfy

$$K(\Phi) \ge Q_2(\Phi) \ge \sup_{c\in(0,1),\, M\in\mathbb{N}^+,\, k\in\mathbb{N}} R(\Phi, M, c, k)\,, \tag{S121}$$

where

$$R(\Phi, M, c, k) := \mathscr{C}(\Phi, c, M)\frac{\prod_{t=0}^{k-1} P_t}{2^k}\mathscr{I}(\alpha_{00}^{(k)}, \alpha_{01}^{(k)}, \alpha_{10}^{(k)}, \alpha_{11}^{(k)})\,. \tag{S122}$$

Fixed $c \in (0,1)$, $M \in \mathbb{N}^+$, and $k \in \mathbb{N}$, the quantities present in (S122) *are defined as follows. $\mathscr{C}(\Phi, c, M)$ is defined as*

$$\mathscr{C}(\Phi, c, M) := \mathrm{Tr}\left[\mathbb{1}_A \otimes \Pi_M\ \mathrm{Id}_A \otimes \Phi(|\Psi_{M,c}\rangle\!\langle\Psi_{M,c}|_{AA'})\right], \tag{S123}$$

where $\Pi_M := |0\rangle\!\langle 0|_B + |M\rangle\!\langle M|_B$ and the state $|\Psi_{M,c}\rangle_{AA'}$ is defined in (S119)*. Let us define for all $m, n \in \{0,1\}$ the coefficients $\alpha_{mn}^{(0)}$ as*

$$\alpha_{mn}^{(0)} := \frac{\langle\psi_{mn}^{(M)}|_{AB}\,\mathbb{1}_A \otimes \Pi_M\ \mathrm{Id}_A \otimes \Phi(|\Psi_{M,c}\rangle\!\langle\Psi_{M,c}|)\,\mathbb{1}_A \otimes \Pi_M\,|\psi_{mn}^{(M)}\rangle_{AB}}{\mathscr{C}(\Phi, c, M)}\,, \tag{S124}$$

where $|\psi^{(M)}_{mn}\rangle_{AB}$ *is defined as*

$$|\psi^{(M)}_{mn}\rangle_{AB} \coloneqq \frac{1}{\sqrt{2}}\sum_{j=0}^{1}(-1)^{mj}\,|jM\rangle_A \otimes |(j\oplus n)M\rangle_B \ . \tag{S125}$$

For all $t\in\{0,1,\ldots,k-1\}$ *and all* $m,n\in\{0,1\}$ *the coefficients* $\alpha^{(t+1)}_{mn}$ *and* P_t *are defined in the following way:*

- *If* $\alpha^{(t)}_{10} < \alpha^{(t)}_{01}$, *then*

$$\alpha^{(t+1)}_{mn} \coloneqq \frac{1}{P_t}\sum_{\substack{m_1,m_2=0\\ m_1\oplus m_2=m}}^{1} \alpha^{(t)}_{m_1 n}\alpha^{(t)}_{m_2 n}\,, \tag{S126}$$

  where

$$P_t \coloneqq \sum_{n=0}^{1}\left(\sum_{m=0}^{1}\alpha^{(t)}_{mn}\right)^2 \ . \tag{S127}$$

- *If* $\alpha^{(t)}_{10} \ge \alpha^{(t)}_{01}$, *then*

$$\alpha^{(t+1)}_{mn} \coloneqq \frac{1}{P_t}\sum_{\substack{n_1,n_2=0\\ n_1\oplus n_2=n}}^{1} \alpha^{(t)}_{m n_1}\alpha^{(t)}_{m n_2}\,, \tag{S128}$$

  where

$$P_t \coloneqq \sum_{m=0}^{1}\left(\sum_{n=0}^{1}\alpha^{(t)}_{mn}\right)^2 \ . \tag{S129}$$

For all $\alpha_{00},\alpha_{01},\alpha_{10},\alpha_{11}\ge 0$ *with* $\alpha_{00}+\alpha_{01}+\alpha_{10}+\alpha_{11}=1$, *the quantity* $\mathscr{I}(\alpha_{00},\alpha_{01},\alpha_{10},\alpha_{11})$ *is defined as*

$$\mathscr{I}(\alpha_{00},\alpha_{01},\alpha_{10},\alpha_{11}) \coloneqq \max\left(Y(\alpha_{00},\alpha_{01},\alpha_{10},\alpha_{11}), Y(\alpha_{00},\alpha_{10},\alpha_{01},\alpha_{11}),\, Y(\alpha_{01},\alpha_{00},\alpha_{10},\alpha_{11})\right)\,, \tag{S130}$$

where the function Y *is defined in* (S21).

Proof. We introduce a protocol to distribute ebits through the channel Φ, which depends on three parameters: $M\in\mathbb{N}^+$, $c\in(0,1)$, $k\in\mathbb{N}$. Our lower bound on $Q_2(\Phi,N_s)$ in (S120) can be obtained by optimising over these parameters the rate of ebits of such a protocol. The lower bound on the other EC two-way capacities follows from (S16). The steps of the protocol are the following.

-Step 1: Alice prepares n_0 copies of the state $|\Psi_{M,c}\rangle_{AA'}$ in (S119) and she sends the halves A' to Bob through the channel Φ. Hence, Alice and Bob share n_0 copies of the state $\mathrm{Id}_A\otimes\Phi(|\Psi_{M,c}\rangle\!\langle\Psi_{M,c}|)$.

-Step 2: Bob performs the local POVM $\{\Pi_M, \mathbb{1}-\Pi_M\}$ on each pair $\mathrm{Id}_A\otimes\Phi(|\Psi_{M,c}\rangle\!\langle\Psi_{M,c}|)$, where $\Pi_M \coloneqq |0\rangle\!\langle 0| + |M\rangle\!\langle M|$. If Bob finds the outcome which corresponds to Π_M, then Alice and Bob keep the pair, otherwise they discard it. They keep the pair with probability

$$\mathscr{C}(\Phi,c,M) \coloneqq \mathrm{Tr}\left[\mathbb{1}_A\otimes\Pi_M\ \mathrm{Id}_A\otimes\Phi(|\Psi_{M,c}\rangle\!\langle\Psi_{M,c}|)\right] \ . \tag{S131}$$

At this point, Alice and Bob shares $\approx n_0\,\mathscr{C}(\Phi,c,M)$ pairs. Each of these pairs are in the state ρ' given by

$$\rho' = \frac{\mathbb{1}_A\otimes\Pi_M\ \mathrm{Id}_A\otimes\Phi(|\Psi_{M,c}\rangle\!\langle\Psi_{M,c}|)\,\mathbb{1}_A\otimes\Pi_M}{\mathscr{C}(\Phi,c,M)} \ . \tag{S132}$$

Note that the support of ρ' is equal to $\mathrm{Span}\{|0\rangle\otimes|0\rangle\,, |0\rangle\otimes|M\rangle\,, |M\rangle\otimes|0\rangle\,, |M\rangle\otimes|M\rangle\}$. For simplicity, in the following we will use the notation $|1\rangle \equiv |M\rangle$. This formally corresponds to consider the state $\rho'' \coloneqq U_M\otimes U_M\,\rho'\,U_M^\dagger\otimes U_M^\dagger$, which is obtained once both Alice and Bob have applied the unitary

$$U_M \coloneqq \sum_{i\neq\{0,M\}}^{\infty} |i\rangle\!\langle i| + |1\rangle\!\langle M| + |M\rangle\!\langle 1| \tag{S133}$$

on the remaining state ρ'. Hence, since the support of ρ'' is equal to $\text{Span}\{|0\rangle\otimes|0\rangle, |0\rangle\otimes|1\rangle, |1\rangle\otimes|0\rangle, |1\rangle\otimes|1\rangle\}$, in the following we consider transformations which act on qubit systems.

-Step 3: For each of the $\approx n_0\,\mathscr{C}(\Phi, c, M)$ pairs, Alice and Bob choose randomly two bits $\mu, \nu \in \{0,1\}$ and they both apply the unitary $\sigma_{\mu\nu}$ defined by

$$\sigma_{\mu\nu} := \sum_{i=0}^{1}(-1)^{\mu i}\,|i\oplus\nu\rangle\!\langle i| \tag{S134}$$

(in terms of the Pauli matrices it holds that $\sigma_{00} = \mathbb{1}_2$, $\sigma_{01} = \sigma_x$, $\sigma_{10} = \sigma_z$, and $\sigma_{11} = i\sigma_y$). Hence, each pair is transformed into the state ρ_0 defined by

$$\rho_0 := \frac{1}{4}\sum_{\mu,\nu=0}^{1}\left(\sigma_{\mu\nu}\otimes\sigma_{\mu\nu}\right)\,\rho''\,\left(\sigma_{\mu\nu}\otimes\sigma_{\mu\nu}\right)^{\dagger}\,. \tag{S135}$$

By exploiting the fact that the Bell states defined in S1 form an orthonormal basis, one can show that ρ is diagonal in the Bell basis:

$$\rho_0 = \sum_{m,n=0}^{1}\alpha_{mn}^{(0)}\,|\psi_{mn}\rangle\!\langle\psi_{mn}|\,, \tag{S136}$$

where the coefficients $\alpha_{mn}^{(0)}$ are given by

$$\alpha_{mn}^{(0)} = \langle\psi_{mn}|\,\rho''\,|\psi_{mn}\rangle = \langle\psi_{mn}^{(M)}|\,\rho'\,|\psi_{mn}^{(M)}\rangle\,, \tag{S137}$$

with $|\psi_{mn}^{(M)}\rangle$ being defined in S125.

-Step 4: Alice and Bob run the following sub-routine, which is a recurrence protocol dubbed *P1-or-P2* [16].

- **Step 4.0**: Let $t = 0$.

- **Step 4.1**: At this point, all the pairs are in the state ρ_t. Alice and Bob collect all the pairs in groups of two pairs. Let $\rho_t^{(A_1B_1)}$ denote the first pair of each group and let $\rho_t^{(A_2B_2)}$ denote the second one. If $\alpha_{10}^{(t)} < \alpha_{01}^{(t)}$, then Alice and Bob apply the bi-local unitary U_1 defined as

$$U_1 := U_{\text{CNOT}}^{(A_1A_2)}\otimes U_{\text{CNOT}}^{(B_1B_2)}\,, \tag{S138}$$

where for all $S = A, B$ the operator $U_{\text{CNOT}}^{(S_1S_2)}$ is the CNOT gate on S_1 and S_2 with control qubit S_1, i.e.

$$U_{\text{CNOT}}^{(S_1S_2)}\,|i\rangle_{S_1}\otimes|j\rangle_{S_2} = |i\rangle_{S_1}\otimes|i\oplus j\rangle_{S_2}\,. \tag{S139}$$

Otherwise if $\alpha_{10}^{(t)} \geq \alpha_{01}^{(t)}$, they apply the bi-local unitary U_2 defined as

$$U_2 := (H^{(A_1)}\otimes H^{(B_1)})(U_{\text{CNOT}}^{(A_1A_2)}\otimes U_{\text{CNOT}}^{(B_1B_2)})(H^{(A_1)}\otimes H^{(A_2)}\otimes H^{(B_1)}\otimes H^{(B_2)})\,, \tag{S140}$$

where for all $S = A_1, A_2, B_1, B_2$ the operator $H^{(S)}$ on S is the Hadamard gate, i.e.

$$H^{(S)} = \frac{1}{\sqrt{2}}\sum_{m,n=0}^{1}(-1)^{mn}\,|n\rangle\!\langle m|_S\,. \tag{S141}$$

At this point, the state of $A_1A_2B_1B_2$ is

$$\rho_t^{(A_1A_2B_1B_2)} := U_p\,\rho_t^{(A_1B_2)}\otimes\rho_k^{(A_2B_2)}\,U_p^{\dagger}\,. \tag{S142}$$

with $p = 1$ if $\alpha_{10}^{(t)} < \alpha_{01}^{(t)}$, and $p = 2$ otherwise.

- **Step 4.2**: Alice and Bob measure the pair A_2B_2 of each group with respect to the local POVM $\{M_{i,j}\}_{i,j\in\{0,1\}}$ with $M_{i,j} := |i\rangle\!\langle i|_{A_2} \otimes |j\rangle\!\langle j|_{B_2}$ for all $i,j \in \{0,1\}$. Then they discard the pair A_2B_2. They discard also the pair A_1B_1 if the outcome of the previous measurement corresponds to $M_{i,j}$ with $i \neq j$. The probability that a pair A_1B_1 is not discarded is given by

$$P_t := \sum_{i=0}^{1} \langle i|_{A_2} \langle i|_{B_2} \operatorname{Tr}_{A_1B_1}\left[\rho_t^{(A_1A_2B_1B_2)}\right] |i\rangle_{A_2} |i\rangle_{B_2} . \tag{S143}$$

By using that for all $k_1, k_2, j_1, j_2 \in \{0,1\}$ it holds that

$$U_{\text{CNOT}}^{(A_1A_2)} \otimes U_{\text{CNOT}}^{(B_1B_2)} |\psi_{k_1j_1}\rangle_{A_1B_1} \otimes |\psi_{k_2j_2}\rangle_{A_2B_2} = |\psi_{k_1\oplus k_2,\, j_1}\rangle_{A_1B_1} \otimes |\psi_{k_2,\, j_1\oplus j_2}\rangle_{A_2B_2} \tag{S144}$$

and that

$$H^{(A)} \otimes H^{(B)} |\psi_{k_1j_1}\rangle_{AB} = (-1)^{k_1j_1} |\psi_{j_1k_1}\rangle_{AB} , \tag{S145}$$

one can show that P_t can be expressed as in (S127) if $\alpha_{10}^{(t)} < \alpha_{01}^{(t)}$, and as in (S129) otherwise. At this point, the number of remaining pairs is

$$\approx n_0\, \mathscr{C}(\Phi, c, M) \frac{1}{2^{t+1}} \prod_{m=0}^{t} P_m \tag{S146}$$

and each of these is in the state ρ_{t+1} given by

$$\rho_{t+1} = \frac{1}{2} \sum_{i=0}^{1} \frac{\langle i|_{A_2} \langle i|_{B_2}\, \rho_t^{(A_1A_2B_1B_2)} |i\rangle_{A_2} |i\rangle_{B_2}}{\operatorname{Tr}_{A_1B_1}\left[\langle i|_{A_2} \langle i|_{B_2}\, \rho_t^{(A_1A_2B_1B_2)} |i\rangle_{A_2} |i\rangle_{B_2}\right]} . \tag{S147}$$

By using (S144) and (S145), one can show that

$$\rho_{t+1} = \sum_{m,n=0}^{1} \alpha_{mn}^{(t+1)} |\psi_{mn}\rangle\!\langle\psi_{mn}| , \tag{S148}$$

where the coefficients $\alpha_{mn}^{(t+1)}$ are given by (S126) if $\alpha_{10}^{(t)} < \alpha_{01}^{(t)}$, and by (S128) otherwise.

- **Step 4.3**: Let $t = t + 1$.

- **Step 4.4**: If the condition $t < k$ is satisfied, then go back to Step 4.1.

Before introducing Step 5, let us recall that if the improved hashing protocol of [17] is applied on states of the form $\rho = \sum_{ij=0}^{1} \alpha_{ij} |\psi_{ij}\rangle\!\langle\psi_{ij}|$ then it can generate ebits with a yield $Y(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11})$ given by (S21). Note that such a yield is not invariant under permutations of the variables $\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}$. Hence, one may achieve a yield which is larger than $Y(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11})$ by applying suitable bi-local unitaries, which suitably permutes the Bell states, just before running the improved hashing protocol. Since the yield function $Y(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11})$ satisfies

$$\begin{aligned} Y(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}) &= Y(\alpha_{10}, \alpha_{01}, \alpha_{00}, \alpha_{11}) , \\ Y(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}) &= Y(\alpha_{00}, \alpha_{11}, \alpha_{10}, \alpha_{01}) , \\ Y(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}) &= Y(\alpha_{01}, \alpha_{00}, \alpha_{11}, \alpha_{10}) , \end{aligned} \tag{S149}$$

then by permuting the four variables α_{ij} it is possible to obtain at most three different values of the rate function, which are: $Y(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11})$, $Y(\alpha_{00}, \alpha_{10}, \alpha_{01}, \alpha_{11})$, and $Y(\alpha_{01}, \alpha_{00}, \alpha_{10}, \alpha_{11})$. Let us define the function $\mathscr{I}$ as

$$\mathscr{I}(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}) := \max\left(Y(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}), Y(\alpha_{00}, \alpha_{10}, \alpha_{01}, \alpha_{11}), Y(\alpha_{01}, \alpha_{00}, \alpha_{10}, \alpha_{11})\right) . \tag{S150}$$

Note that at the beginning of Step 5, the number of remaining pairs is

$$\approx n_0\, \mathscr{C}(\Phi, c, M) \frac{1}{2^k} \prod_{t=0}^{k-1} P_t \tag{S151}$$

and each of these is in $\rho_k = \sum_{m,n=0}^{1} \alpha_{mn}^{(k)} |\psi_{mn}\rangle\!\langle\psi_{mn}|$.

-Step 5: If $\mathscr{I}(\alpha_{00}^{(k)},\alpha_{01}^{(k)},\alpha_{10}^{(k)},\alpha_{11}^{(k)}) = Y(\alpha_{00}^{(k)},\alpha_{10}^{(k)},\alpha_{01}^{(k)},\alpha_{11}^{(k)})$, then both Alice and Bob apply the Hadamard gate defined by (S141). Therefore, in this case, the state of each of pairs becomes

$$(H\otimes H)\,\rho_k\,(H\otimes H)^\dagger = \alpha_{00}^{(k)}\,|\psi_{00}\rangle\!\langle\psi_{00}| + \alpha_{10}^{(k)}\,|\psi_{01}\rangle\!\langle\psi_{01}| + \alpha_{01}^{(k)}\,|\psi_{10}\rangle\!\langle\psi_{10}| + \alpha_{11}^{(k)}\,|\psi_{11}\rangle\!\langle\psi_{11}|\,, \tag{S152}$$

where we have exploited (S145). If $\mathscr{I}(\alpha_{00}^{(k)},\alpha_{01}^{(k)},\alpha_{10}^{(k)},\alpha_{11}^{(k)}) = Y(\alpha_{01}^{(k)},\alpha_{00}^{(k)},\alpha_{10}^{(k)},\alpha_{11}^{(k)})$, then both Alice and Bob apply $B_x := \frac{\mathbb{1}_2 - i\sigma_{01}}{\sqrt{2}}$, where σ_{01} is defined by (S134), and hence the state becomes

$$(B_x\otimes B_x)\,\rho_k\,(B_x\otimes B_x)^\dagger = \alpha_{01}^{(k)}\,|\psi_{00}\rangle\!\langle\psi_{00}| + \alpha_{00}^{(k)}\,|\psi_{01}\rangle\!\langle\psi_{01}| + \alpha_{10}^{(k)}\,|\psi_{10}\rangle\!\langle\psi_{10}| + \alpha_{11}^{(k)}\,|\psi_{11}\rangle\!\langle\psi_{11}|\,. \tag{S153}$$

-Step 6: Alice and Bob run the improved hashing protocol of [17], which can achieve the yield $\mathscr{I}(\alpha_{00}^{(k)},\alpha_{01}^{(k)},\alpha_{10}^{(k)},\alpha_{11}^{(k)})$. Hence, in the end, Alice and Bob can generate a number of ebits equal to

$$\approx n_0\,\mathscr{C}(\Phi,c,M)\frac{\prod_{t=0}^{k-1}P_t}{2^k}\mathscr{I}(\alpha_{00}^{(k)},\alpha_{01}^{(k)},\alpha_{10}^{(k)},\alpha_{11}^{(k)})\,. \tag{S154}$$

Since the channel Φ is used n_0 times (during Step 1) to send the n_0 halves of the state $|\Psi_{M,c}\rangle_{AA'}$, the rate of distributed ebits of the presented protocol is

$$\mathscr{C}(\Phi,c,M)\frac{\prod_{t=0}^{k-1}P_t}{2^k}\mathscr{I}(\alpha_{00}^{(k)},\alpha_{01}^{(k)},\alpha_{10}^{(k)},\alpha_{11}^{(k)})\,. \tag{S155}$$

Since the local mean photon number of $|\Psi_{M,c}\rangle_{AA'}$ is $(1-c^2)M$, the rate in (S155) is a lower bound on the energy-constrained two-way quantum capacity $Q_2(\Phi,N_s)$ for all $M\in\mathbb{N}^+$, $c\in(0,1)$, $k\in\mathbb{N}$ such that $(1-c^2)M\le N_s$. The optimisation over these parameters of the rate in (S155) leads to the lower bound on $Q_2(\Phi,N_s)$ in (S120). In addition, since $K(\Phi,N_s)\ge Q_2(\Phi,N_s)$ thanks to (S16), we have proved (S120). By taking the limit $N_s\to\infty$ of (S120), the lower bound on the unconstrained two-way capacities in (S121) is also proved. □

In the forthcoming Theorem S14 we apply Theorem S13 to the composition $\mathscr{N}_{g,\lambda} := \Phi_{g,0}\circ\mathscr{E}_{\lambda,0}$ between pure amplifier channel $\Phi_{g,0}$ and pure loss channel $\mathscr{E}_{\lambda,0}$.

Theorem S14. *Let $g\ge 1$, $\lambda\in[0,1]$, and $N_s\ge 0$. The EC two-way capacities $Q_2(\mathscr{N}_{g,\lambda},N_s)$ and $K(\mathscr{N}_{g,\lambda},N_s)$ of the composition $\mathscr{N}_{g,\lambda} := \Phi_{g,0}\circ\mathscr{E}_{\lambda,0}$ between pure amplifier channel and pure loss channel satisfy the following lower bound*

$$K(\mathscr{N}_{g,\lambda},N_s)\ge Q_2(\mathscr{N}_{g,\lambda},N_s)\ge \sup_{\substack{c\in(0,1),\,M\in\mathbb{N}^+,\,k\in\mathbb{N}\\(1-c^2)M\le N_s}} \mathscr{R}(g,\lambda,M,c,k)\,, \tag{S156}$$

and, in particular, the unconstrained two-way capacities satisfy

$$K(\mathscr{N}_{g,\lambda})\ge Q_2(\mathscr{N}_{g,\lambda})\ge \sup_{c\in(0,1),\,M\in\mathbb{N}^+,\,k\in\mathbb{N}} \mathscr{R}(g,\lambda,M,c,k)\,, \tag{S157}$$

where

$$\mathscr{R}(g,\lambda,M,c,k) := R(\mathscr{N}_{g,\lambda},M,c,k)\,, \tag{S158}$$

with the quantity $R(\mathscr{N}_{g,\lambda},M,c,k)$ being defined in Theorem S13. The quantities $\mathscr{C}(\mathscr{N}_{g,\lambda},c,M)$ and $\alpha_{mn}^{(0)}$, which appear in the definition of $R(\mathscr{N}_{g,\lambda},M,c,k)$ in Theorem S13, can be expressed as

$$\begin{aligned}\mathscr{C}(\mathscr{N}_{g,\lambda},c,M) &:= \sum_{n,l=0}^{1} c_n^2\, f_{Mn,Mn,Ml}(g,\lambda)\,,\\ \alpha_{mn}^{(0)} &:= \frac{1}{2\mathscr{C}(\mathscr{N}_{g,\lambda},c,M)}\sum_{x,y=0}^{1}\sum_{l=\max(y-x,0)}^{1+\min(y-x,0)} \delta_{x\oplus n,l+x-y}\,\delta_{y\oplus n,l}\,(-1)^{m(x+y)}c_xc_y\,f_{Mx,My,Ml}(g,\lambda)\,,\end{aligned} \tag{S159}$$

where $c_0 := c$, $c_1 := \sqrt{1-c^2}$, $f_{n,i,l}(g,\lambda)$ is defined in (S79)*, and $\delta_{x,y}$ denotes the Kronecker delta.*

Proof. (S156) and (S157) follows by applying Theorem S13 to $\mathcal{N}_{g,\lambda}$. We only need to show the expressions of $\mathscr{C}(\mathcal{N}_{g,\lambda}, c, M)$ and $\alpha_{mn}^{(0)}$ in (S159). In this proof we use the notation introduced in the statement of Theorem S13. By using (S78), we deduce that

$$\mathrm{Id}_A \otimes \mathcal{N}_{g,\lambda}(|\Psi_{M,c}\rangle\!\langle\Psi_{M,c}|) = \sum_{n,i=0}^{1} \sum_{l=M\max(i-n,0)}^{\infty} c_n c_i f_{Mn,Mi,l}(g,\lambda)\, |Mn\rangle\!\langle Mi|_A \otimes |l+M(n-i)\rangle\!\langle l|_B \,. \tag{S160}$$

Consequently, it holds that

$$\mathbb{1}_A \otimes \Pi_M \ \mathrm{Id}_A \otimes \mathcal{N}_{g,\lambda}(|\Psi_{M,c}\rangle\!\langle\Psi_{M,c}|)\, \mathbb{1}_A \otimes \Pi_M = \sum_{n,i=0}^{1} \sum_{l=\max(i-n,0)}^{1+\min(i-n,0)} c_n c_i f_{Mn,Mi,Ml}(g,\lambda)\, |Mn\rangle\!\langle Mi|_A \otimes |M(l+n-i)\rangle\!\langle Ml|_B \,. \tag{S161}$$

By inserting this into the definition of $\mathscr{C}(\mathcal{N}_{g,\lambda}, c, M)$ in (S123) and of $\alpha_{mn}^{(0)}$ in (S124), one obtains the expressions in (S159). □

B. Remarks

Let us consider the entanglement distribution protocol shown in the proof of Theorem S13 applied to the the composition $\mathcal{N}_{g,\lambda} := \Phi_{g,0} \circ \mathscr{E}_{\lambda,0}$ between pure amplifier channel $\Phi_{g,0}$ and pure loss channel $\mathscr{E}_{\lambda,0}$. After completing Step 2 of this protocol, the entanglement distribution process is reduced to an entanglement distillation protocol on the two-qubit state reported in (S132). We will denote this two-qubit state as $\rho_{AB}^{(g,\lambda,M,c)}$, where $M \in \mathbb{N}^+$ and $c \in (0,1)$ correspond to the constants appearing in the state in (S119) that Alice produces during Step 1. The natural question that arises is: "Under what conditions is $\rho_{AB}^{(g,\lambda,M,c)}$ distillable?" In Remark 1 we answer this question.

Remark 1. *$\rho_{AB}^{(g,\lambda,M,c)}$ is distillable if and only if λ and g satisfy the inequality $(1-\lambda)g < 1$, meaning that $\mathcal{N}_{g,\lambda}$ is not entanglement breaking. This provides an alternative proof of Theorem S12.*

Proof. By exploiting (S161), for all $g > 1, \lambda \in (0,1), M \in \mathbb{N}^+, c \in (0,1)$ the state in (S132) can be expressed as

$$\rho_{AB}^{(g,\lambda,M,c)} := \frac{\sum_{n,i=0}^{1} \sum_{l=\max(i-n,0)}^{1+\min(i-n,0)} c_n c_i f_{Mn,Mi,Ml}(g,\lambda)\, |Mn\rangle\!\langle Mi|_A \otimes |M(l+n-i)\rangle\!\langle Ml|_B}{\sum_{n,l=0}^{1} c_n^2\, f_{Mn,Mn,Ml}(g,\lambda)} \,, \tag{S162}$$

where $c_0 := c$, $c_1 := \sqrt{1-c^2}$, and $f_{n,i,l}(g,\lambda)$ is defined in (S79). Consequently, it holds that

$$\begin{aligned}\rho_{AB}^{(g,\lambda,M,c)} = \frac{1}{\sum_{n,l=0}^{1} c_n^2\, f_{Mn,Mn,Ml}(g,\lambda)} \big[& c^2 f_{0,0,0}(g,\lambda)\, |0\rangle\!\langle 0|_A \otimes |0\rangle\!\langle 0|_B \\ & + c^2 f_{0,0,M}(g,\lambda)\, |0\rangle\!\langle 0|_A \otimes |M\rangle\!\langle M|_B \\ & + c\sqrt{1-c^2} f_{0,M,M}(g,\lambda)\, |0\rangle\!\langle M|_A \otimes |0\rangle\!\langle M|_B \\ & + c\sqrt{1-c^2} f_{M,0,0}(g,\lambda)\, |M\rangle\!\langle 0|_A \otimes |M\rangle\!\langle 0|_B \\ & + (1-c^2) f_{M,M,0}(g,\lambda)\, |M\rangle\!\langle M|_A \otimes |0\rangle\!\langle 0|_B \\ & + (1-c^2) f_{M,M,M}(g,\lambda)\, |M\rangle\!\langle M|_A \otimes |M\rangle\!\langle M|_B \big] \,,\end{aligned} \tag{S163}$$

Hence, the matrix associated with the partial transpose on B of $\rho_{AB}^{(g,\lambda,M,c)}$, written with respect the basis $\{|0\rangle_A \otimes |0\rangle_B\,, |0\rangle_A \otimes |M\rangle_B\,, |M\rangle_A \otimes |0\rangle_B\,, |M\rangle_A \otimes |M\rangle_B\}$, is

$$\frac{1}{\sum_{n,l=0}^{1} c_n^2\, f_{Mn,Mn,Ml}(g,\lambda)} \begin{pmatrix} c^2 f_{0,0,0}(g,\lambda) & 0 & 0 & 0 \\ 0 & c^2 f_{0,0,M}(g,\lambda) & c\sqrt{1-c^2} f_{0,M,M}(g,\lambda) & 0 \\ 0 & c\sqrt{1-c^2} f_{M,0,0}(g,\lambda) & (1-c^2) f_{M,M,0}(g,\lambda) & 0 \\ 0 & 0 & 0 & (1-c^2) f_{M,M,M}(g,\lambda) \end{pmatrix} .$$

It follows that $\rho_{AB}^{(g,\lambda,M,c)}$ is not PPT if and only if

$$f_{M,0,0}(g,\lambda)\, f_{M,M,0}(g,\lambda) < f_{0,M,M}(g,\lambda)\, f_{0,0,M}(g,\lambda) \,. \tag{S164}$$

The definition of $f_{\cdot,\cdot,\cdot}(g,\lambda)$ in (S79) yields

$$\begin{aligned} f_{0,0,M}(g,\lambda) &= \frac{(g-1)^M}{g^{1+M}}\,, \\ f_{M,M,0}(g,\lambda) &= \frac{(1-\lambda)^M}{g}\,, \\ f_{0,M,M}(g,\lambda) &= f_{M,0,0}(g,\lambda) = \frac{\lambda^{\frac{M}{2}}}{g^{1+\frac{M}{2}}}\,. \end{aligned} \tag{S165}$$

Consequently, (S164) establishes that $\rho_{AB}^{(g,\lambda,M,c)}$ is not PPT if and only if $(1-\lambda)g<1$, independentely of c and M. The fact that any two-qubit state is distillable if and only if it is not PPT [36] implies that $\rho_{AB}^{(g,\lambda,M,c)}$ is distillable if and only if $(1-\lambda)g<1$ for all $c\in(0,1)$ and all $M\in\mathbb{N}^+$.

Let us now show that this fact constitutes an alternative proof of Theorem S12, i.e. let us show that the energy-constrained two-way capacities $Q_2(\mathcal{N}_{g,\lambda},N_s)$ and $K(\mathcal{N}_{g,\lambda},N_s)$ are strictly positive if and only if $(1-\lambda)g<1$, i.e. if and only if $\mathcal{N}_{g,\lambda}$ is not entanglement breaking. The entanglement distribution protocol's Steps S1 and S2 imply that for all $N_s\ge 0$ it holds that $Q_2(\mathcal{N}_{g,\lambda},N_s)\ge E_d\left(\rho_{AB}^{(g,\lambda,M,c)}\right)$, for any $c\in(0,1)$ and $M\in\mathbb{N}^+$ satisfying $(1-c^2)M\le N_s$. Here, $E_d(\cdot)$ denotes the distillable entanglement. As we have proved above, if $(1-\lambda)g<1$ then the state $\rho_{AB}^{(g,\lambda,M,c)}$ is distillable, i.e. $E_d(\rho_{AB}^{(g,\lambda,M,c)})>0$. This implies that if $(1-\lambda)g<1$, then the energy-constrained two-way capacities of $\mathcal{N}_{g,\lambda}$ are strictly positive, i.e. $K(\mathcal{N}_{g,\lambda},N_s)\ge Q_2(\mathcal{N}_{g,\lambda},N_s)>0$. Conversely, by exploiting Theorem S3 and the fact that any entanglement-breaking channel has vanishing two-way capacities, it follows that if $(1-\lambda)g\ge 1$ then $K(\mathcal{N}_{g,\lambda})=Q_2(\mathcal{N}_{g,\lambda})=0$ and hence $K(\mathcal{N}_{g,\lambda},N_s)=Q_2(\mathcal{N}_{g,\lambda},N_s)=0$. □

Remark 1 ensures that if the channel $\mathcal{N}_{g,\lambda}$ is not entanglement breaking, then the state $\rho_{AB}^{(g,\lambda,M,c)}$ obtained at the end of Step 2 is distillable for any $M\in\mathbb{N}^+$ and $c\in(0,1)$. We now turn our attention to the state, denoted as $\sigma_{AB}^{(g,\lambda,M,c)}$, which is obtained at the end of Step 3 through Pauli-based twirling of $\rho_{AB}^{(g,\lambda,M,c)}$. It is possible for this operation to map distillable states to undistillable states, so we ask the question: "Under what conditions is $\sigma_{AB}^{(g,\lambda,M,c)}$ distillable?" In Remark 2 we will demonstrate that for any $\lambda\in(0,1)$ and $g>1$, if $\mathcal{N}_{g,\lambda}$ is not entanglement breaking, then for all $M\in\mathbb{N}^+$ the state $\sigma_{AB}^{(g,\lambda,M,\bar{c})}$ is distillable, where $\bar{c}:=\frac{1}{\sqrt{1+(g-1)^M}}$. This means that Alice and Bob can choose the value of c appropriately such that the Pauli-based twirling does not affect the distillability of the shared state.

Remark 2. *Let $M\in\mathbb{N}^+$, $\lambda\in(0,1)$, and $g>1$ with $(1-\lambda)g<1$ (meaning that $\mathcal{N}_{g,\lambda}$ is not entanglement breaking). Then, the state $\sigma_{AB}^{(g,\lambda,M,\bar{c})}$ is distillable, where $\bar{c}:=\frac{1}{\sqrt{1+(g-1)^M}}$.*

Proof. After applying the Pauli-based twirling on the state $\rho_{AB}^{(g,\lambda,M,\bar{c})}$, the resulting state $\sigma_{AB}^{(g,\lambda,M,\bar{c})}$ is transformed into a Bell-diagonal form, that is

$$\sigma_{AB}^{(g,\lambda,M,\bar{c})} = \sum_{i,j=0}^{1} p_{ij}\,|\psi_{ij}^{(M)}\rangle\!\langle\psi_{ij}^{(M)}|_{AB}\,, \tag{S166}$$

where $p_{ij}:=\langle\psi_{ij}^{(M)}|\,\rho_{AB}^{(g,\lambda,M,\bar{c})}\,|\psi_{ij}^{(M)}\rangle$ and $\{|\psi_{ij}^{(M)}\rangle_{AB}\}_{i,j\in\{0,1\}}$ are the Bell states defined in (S125). In particular, it holds that

$$\begin{aligned} p_{00}+p_{10} &= \langle 0|_A\langle 0|_B\,\rho_{AB}^{(g,\lambda,M,c)}\,|0\rangle_A|0\rangle_B + \langle M|_A\langle M|_B\,\rho_{AB}^{(g,\lambda,M,c)}\,|M\rangle_A|M\rangle_B\,, \\ p_{01}-p_{11} &= 2\,\langle 0|_A\langle 0|_B\,\rho_{AB}^{(g,\lambda,M,c)}\,|M\rangle_A|M\rangle_B\,, \\ p_{01}+p_{11} &= \langle 0|_A\langle M|_B\,\rho_{AB}^{(g,\lambda,M,c)}\,|0\rangle_A|M\rangle_B + \langle M|_A\langle 0|_B\,\rho_{AB}^{(g,\lambda,M,c)}\,|M\rangle_A|0\rangle_B\,, \\ p_{00}-p_{10} &= 2\,\langle 0|_A\langle 0|_B\,\rho_{AB}^{(g,\lambda,M,c)}\,|M\rangle_A|M\rangle_B\,. \end{aligned} \tag{S167}$$

Lemma S15 guarantees that if $p_{01}+p_{11}-|p_{00}-p_{10}|<0$ then the state $\sigma_{AB}^{(g,\lambda,M,\bar{c})}$ is distillable. By using (S163) and (S167), the condition $p_{01}+p_{11}-|p_{00}-p_{10}|<0$ is satisfied if and only if

$$\bar{c}^2 f_{0,0,M}(g,\lambda) + (1-\bar{c}^2) f_{M,M,0}(g,\lambda) - 2\bar{c}\sqrt{1-\bar{c}^2}\,f_{M,0,0}(g,\lambda) < 0\,, \tag{S168}$$

that is

$$\bar{c}^2(g-1)^M + (1-\bar{c}^2)(1-\lambda)^M g^M - 2\bar{c}\sqrt{1-\bar{c}^2}(\lambda g)^{M/2} < 0\,, \tag{S169}$$

where we have exploited (S165). By hypothesis, the channel $\mathcal{N}_{g,\lambda}$ is entanglement breaking and hence $(1-\lambda)g < 1$, as established by Lemma S4. Consequently, for all $g > 1$ and $\lambda \in (0,1)$ it holds that

$$\begin{aligned}\bar{c}^2(g-1)^M + (1-\bar{c}^2)(1-\lambda)^M g^M - 2\bar{c}\sqrt{1-\bar{c}^2}(\lambda g)^{M/2} &< \bar{c}^2(g-1)^M + (1-\bar{c}^2) - 2\bar{c}\sqrt{1-\bar{c}^2}(g-1)^{M/2} \\ &= \left(\bar{c}(g-1)^{M/2} - \sqrt{1-\bar{c}^2}\right)^2 = 0\,,\end{aligned} \tag{S170}$$

where we have used that $\bar{c} := \frac{1}{\sqrt{1+(g-1)^M}}$. Hence, for all $M \in \mathbb{N}^+$, $\lambda \in (0,1)$, and $g > 1$ with $(1-\lambda)g < 1$, it holds that $\sigma_{AB}^{(g,\lambda,M,\bar{c})}$ is distillable. □

Lemma S15. *Let* $\{|\psi_{ij}\rangle\}_{i,j\in\{0,1\}}$ *be the Bell states defined in* (S1). *A convex combination of Bell states* $\rho_{AB} = \sum_{i,j=0}^1 p_{ij}\,|\psi_{ij}\rangle\!\langle\psi_{ij}|$ *is distillable if and only if* $p_{00}+p_{10} < |p_{01}-p_{10}|$ *or* $p_{01}+p_{11} < |p_{00}-p_{10}|$.

Proof. The matrix associated with $\rho_{AB} = \sum_{i,j=0}^1 p_{ij}\,|\psi_{ij}\rangle\!\langle\psi_{ij}|$, written with respect the basis $\{|0\rangle_A \otimes |0\rangle_B\,, |0\rangle_A \otimes |1\rangle_B\,, |1\rangle_A \otimes |0\rangle_B\,, |1\rangle_A \otimes |1\rangle_B\}$, is

$$\frac{1}{2}\begin{pmatrix} p_{00}+p_{10} & 0 & 0 & p_{00}-p_{10} \\ 0 & p_{10}+p_{11} & p_{10}-p_{11} & 0 \\ 0 & p_{10}-p_{11} & p_{10}+p_{11} & 0 \\ p_{00}-p_{10} & 0 & 0 & p_{00}+p_{10} \end{pmatrix}.$$

Its partial transpose on B is

$$\frac{1}{2}\begin{pmatrix} p_{00}+p_{10} & 0 & 0 & p_{10}-p_{11} \\ 0 & p_{10}+p_{11} & p_{00}-p_{10} & 0 \\ 0 & p_{00}-p_{10} & p_{10}+p_{11} & 0 \\ p_{10}-p_{11} & 0 & 0 & p_{00}+p_{10} \end{pmatrix}.$$

Hence, the state ρ_{AB} is PPT if and only if $p_{00}+p_{10} \geq |p_{01}-p_{10}|$ and $p_{01}+p_{11} \geq |p_{00}-p_{10}|$. Consequently, the fact that any two-qubit state is distillable if and only if it is not PPT [36] implies the validity of the thesis. □

C. Experimental challenges regarding our protocol

As demonstrated in the main text, applying our main result regarding the maximum tolerable excess noise to the current Internet infrastructure shows that continuous-variable quantum key distribution is feasible if and only if the fibre length is approximately less than 1000 kilometres. Hence, any practical QKD protocol, which is based on the existing Internet infrastructure, must adhere to this fundamental limit. Furthermore, this limit of 1000 kilometres can now serve as a benchmark for evaluating the quality of any new CV-QKD protocol, underscoring the significant impact of our results on practical implementations.

The potential benefit of our protocol (presented both in the main text and in the proof of Theorem S13 above) lies in its *faithfulness* — it can distil entanglement (and hence generate secret keys) whenever the channel is not entanglement breaking. With the current Internet infrastructure based on optical fibres, our protocol could *theoretically* achieve the ultimate limit set by quantum physics of transmitting entanglement and secret keys over distances up to 1000 kilometres. This is a unique feature of our protocol, which stands in stark contrast with *all* existing entanglement distribution and key distribution protocols.

While there exist CV-QKD protocols that are relatively easy to implement with current technology (capable of distributing secret keys across optical fibres of at most 200 kilometres [37–41]), this is not the case for entanglement distribution. Indeed, *all* known entanglement-distribution protocols are experimentally challenging with current technology. For example, the best known entanglement-distribution protocol prior to our work [22] — i.e. the hashing protocol applied to the Choi state of the channel — is not experimentally feasible.

Our protocol is an entanglement-distribution protocol and, as such, is experimentally challenging at present. We emphasise that this limitation is not unique to our protocol but is a common challenge faced by *all* entanglement distribution protocols due to current technological constraints. A major factor is the lack of a noiseless quantum memory, which makes it challenging to perform even a few iterations of a recurrence entanglement distillation protocol. Nevertheless, given the significant recent experimental advancements regarding quantum memories [42, 43] and entanglement distillation [44–46], we are optimistic about the future experimental viability of our protocol. Hence, we stress that, although our protocol is experimentally challenging with current technology, there is no way that a protocol as simple as our ours will *not* be realisable in a few decades at worst.

Let us provide further details about a possible practical realisation of our protocol. To perform Step 1, it suffices that Alice produces the state

$$|\Psi\rangle_{AA'} := \frac{|0\rangle_A \otimes |0\rangle_{A'} + |1\rangle_A \otimes |1\rangle_{A'}}{\sqrt{2}} \tag{S171}$$

in order to make the rate of the protocol faithful. However, without changing the rate (as explained below), Alice can instead produce the *NOON state* [47]

$$|\Psi'\rangle_{AA'} := \frac{|0\rangle_A \otimes |1\rangle_{A'} + |1\rangle_A \otimes |0\rangle_{A'}}{\sqrt{2}} , \tag{S172}$$

which can be experimentally prepared [48, 49]. After Alice has sent the sub-system A' through the channel to Bob, Step 2 involves performing a non-demolition measurement with the POVM operator $|0\rangle\!\langle 0|_B + |1\rangle\!\langle 1|_B$. Although this measurement appears challenging to implement experimentally, fortunately the problem has been studied already, and several promising approaches do exist. Specifically, one may exploit either: the pre-certification scheme employed in [50]; the coupling scheme between optical signals and trapped cold atomic gas designed in [51]; single photon filters based on Rydberg blockade [52, 53] to implement single photon subtraction [54, 55]; single atoms inside an optical cavity to perform single photon subtraction [56, 57]. After this non-demolition measurement, Alice and Bob share a two-mode state in the subspace spanned by $\{|0\rangle \otimes |0\rangle , |0\rangle \otimes |1\rangle , |1\rangle \otimes |0\rangle , |1\rangle \otimes |1\rangle\}$. At this point, they can transfer their state from the optical modes to a qubit solid-state platform (e.g., superconducting or trapped ion platform). This transfer can be experimentally performed in several ways, for example by exploiting: the quantum-memory based approaches introduced in [42, 43]; the aforementioned single photon subtraction methods [52–57], which map the photonic state onto the atomic state; quantum transduction from optical to microwave photons that are compatible with the superconducting qubits [58–60]. This means that only the first two steps of the protocol involve optical platforms, which is advantageous because all the two-qubit unitaries used in the subsequent steps of our protocol are much easier to experimentally implement in a qubit platform. To address the fact that Alice has sent the NOON state in (S172) instead of the state in (S171), she simply needs to apply the Pauli σ_x before initiating Step 3.

IV. MULTI-RAIL STRATEGIES

In this section we introduce an additional protocol for distributing ebits across the piBGC $\mathcal{N}_{g,\lambda}$ by combining and optimising the multi-rail protocol introduced in [61] and the qudit P1-or-P2 protocol introduced in [16]. To begin, we will establish some notation and we will prove a useful lemma. For any $K \in \mathbb{N}$ with $K \geq 2$ and any $\mathbf{n} := (n_1, \ldots, n_K) \in \mathbb{N}^K$, we denote as $|\mathbf{n}\rangle_{A_1 \ldots A_K}$ the following K-mode Fock state with total photon number equal to $\|\mathbf{n}\|_1$:

$$|\mathbf{n}\rangle_{A_1 \ldots A_K} := |n_1\rangle_{A_1} \otimes |n_2\rangle_{A_2} \otimes \ldots \otimes |n_K\rangle_{A_K} , \tag{S173}$$

where we have used the notation $\|\mathbf{n}\|_1 := \sum_{j=1}^{K} n_j$. For any $N, K \in \mathbb{N}^+$ with $K \geq 2$, let us order the set

$$\{|\mathbf{n}\rangle_{A_1 \ldots A_K} : \mathbf{n} \in \mathbb{N}^K , \|\mathbf{n}\|_1 = N\} \tag{S174}$$

according to the restricted lexicographic ordering. More formally, the relation $\preceq$ is defined as

$$|\mathbf{n}\rangle_{A_1 \ldots A_K} \preceq |\mathbf{m}\rangle_{A_1 \ldots A_K} \Longleftrightarrow \sum_{j=1}^{K} n_j \,(N+1)^j < \sum_{j=1}^{K} m_j \,(N+1)^j . \tag{S175}$$

The set has $\binom{N+K-1}{N}$ elements, and for all $n=0,1,\ldots,\binom{N+K-1}{N}-1$, we define the state $|\phi_n^{(N)}\rangle_{A_1\ldots A_K}$ as the nth element of the ordered set. For example, if $N=2$ and $K=3$, we have that

$$\begin{aligned}
|\phi_0^{(2)}\rangle_{A_1A_2A_3} &:= |0\rangle_{A_1}\otimes|0\rangle_{A_2}\otimes|2\rangle_{A_3}\,,\\
|\phi_1^{(2)}\rangle_{A_1A_2A_3} &:= |0\rangle_{A_1}\otimes|1\rangle_{A_2}\otimes|1\rangle_{A_3}\,,\\
|\phi_2^{(2)}\rangle_{A_1A_2A_3} &:= |0\rangle_{A_1}\otimes|2\rangle_{A_2}\otimes|0\rangle_{A_3}\,,\\
|\phi_3^{(2)}\rangle_{A_1A_2A_3} &:= |1\rangle_{A_1}\otimes|0\rangle_{A_2}\otimes|1\rangle_{A_3}\,,\\
|\phi_4^{(2)}\rangle_{A_1A_2A_3} &:= |1\rangle_{A_1}\otimes|1\rangle_{A_2}\otimes|0\rangle_{A_3}\,,\\
|\phi_5^{(2)}\rangle_{A_1A_2A_3} &:= |2\rangle_{A_1}\otimes|0\rangle_{A_2}\otimes|0\rangle_{A_3}\,.
\end{aligned} \tag{S176}$$

In addition, for all $N,K\in\mathbb{N}^+$ with $K\ge 2$ let us define the following state of $K+K$ modes $A_1,\ldots,A_k,A'_1,\ldots,A'_K$:

$$\begin{aligned}
|\Psi_{N,K}\rangle_{A_1\ldots A_K,A'_1,\ldots,A'_K} &:= \frac{1}{\sqrt{\binom{N+K-1}{N}}}\sum_{n=0}^{\binom{N+K-1}{N}-1} |\phi_n^{(N)}\rangle_{A_1\ldots A_k}\otimes|\phi_n^{(N)}\rangle_{A'_1\ldots A'_k}\\
&= \frac{1}{\sqrt{\binom{N+K-1}{N}}}\sum_{\substack{\mathbf{n}\in\mathbb{N}^K\\ \|\mathbf{n}\|_1=N}} |\mathbf{n}\rangle_{A_1\ldots A_K}\otimes|\mathbf{n}\rangle_{A'_1\ldots A'_K}\,,
\end{aligned} \tag{S177}$$

which is a $\binom{N+K-1}{N}$-dimensional maximally entangled state that corresponds to the subspace of the Hilbert space of K modes with total photon number equal to N. Moreover, let us define for all $K,F\in\mathbb{N}$ the projector $\Pi_F^{(K)}$ onto the subspace of K modes $A_1,\ldots,A_K$ whose total photon number equals F, i.e.

$$\Pi_F^{(K)} := \sum_{\substack{\mathbf{m}\in\mathbb{N}^K\\ \|\mathbf{m}\|_1=F}} |\mathbf{m}\rangle\!\langle\mathbf{m}|_{A_1\ldots A_K}\,. \tag{S178}$$

The following lemma will be useful in order to calculate the rate of our entanglement distribution protocol.

Lemma S16. *Let $\lambda\in[0,1], g\ge 1, N\in\mathbb{N}, K\in\mathbb{N}^+$, and $\boldsymbol{n}\in\mathbb{N}^K$ such that $\|\boldsymbol{n}\|_1=N$. Assume that Alice transmits the K-mode Fock state $|\boldsymbol{n}\rangle$ to Bob via K parallel uses of the piBGC $\mathcal{N}_{g,\lambda}:=\Phi_{g,0}\circ\mathcal{E}_{\lambda,0}$ and suppose further that Bob measures the total photon number of the K received modes. The probability $\mathscr{P}_F$ that Bob gets the outcome $F\in\mathbb{N}$ is*

$$\mathscr{P}_F := \mathrm{Tr}\left[\mathcal{N}_{g,\lambda}^{\otimes K}(|\boldsymbol{n}\rangle\!\langle\boldsymbol{n}|)\,\Pi_F^{(K)}\right] = \sum_{P=0}^{\min(F,N)}\binom{N}{P}\binom{K+F-1}{F-P}\lambda^P(1-\lambda)^{N-P}\frac{(g-1)^{F-P}}{g^{K+F}}\,. \tag{S179}$$

In particular, note that $\mathscr{P}_F$ depends on $\boldsymbol{n}$ only through the total photon number $\|\boldsymbol{n}\|_1=N$. Specifically, if the communication channel is the pure loss channel $\mathcal{E}_{\lambda,0}=\mathcal{N}_{1,\lambda}$, the probability of getting the outcome $F\in\mathbb{N}$ is

$$\mathrm{Tr}\left[\mathcal{E}_{\lambda,0}^{\otimes K}(|\boldsymbol{n}\rangle\!\langle\boldsymbol{n}|)\,\Pi_F^{(K)}\right] = \binom{N}{F}\lambda^F(1-\lambda)^{N-F}\Theta(N-F)\,, \tag{S180}$$

where we have introduced the Heaviside function $\Theta(x)$ defined as $\Theta(x)=1$ if $x\ge 0$, and $\Theta(x)=0$ if $x<0$. In addition, if the communication channel is the pure amplifier channel $\Phi_{g,0}=\mathcal{N}_{g,1}$, the probability of getting the outcome $F\in\mathbb{N}$ is

$$\mathrm{Tr}\left[\Phi_{g,0}^{\otimes K}(|\boldsymbol{n}\rangle\!\langle\boldsymbol{n}|)\,\Pi_F^{(K)}\right] = \binom{K+F-1}{F-N}\frac{(g-1)^{F-N}}{g^{K+F}}\Theta(F-N)\,. \tag{S181}$$

Therefore, the probability $\mathscr{P}_F$ in (S179) *of getting F photons at the output of K parallel uses of the composition between pure loss channel and pure amplifier channel can be expressed as the sum over $P\in\mathbb{N}$ of the conditional probability of getting F photons at the output of the K pure amplifier channels conditioned on the event of getting P photons at the output of the K pure loss channels, multiplied by the probability of the latter event.*

Proof. As a consequence of (S98), for all $n \in \mathbb{N}$ it holds that

$$\mathscr{E}_{\lambda,0}(|n\rangle\langle n|) = \sum_{l=0}^{n} \binom{n}{l} \lambda^l (1-\lambda)^{n-l} \, |l\rangle\langle l| \tag{S182}$$

and hence

$$\mathscr{E}_{\lambda,0}^{\otimes K}(|\mathbf{n}\rangle\langle\mathbf{n}|) = \sum_{\substack{\mathbf{l}\in\mathbb{N}^K \\ \mathbf{l}\le\mathbf{n}}} \left(\prod_{j=1}^{K} \binom{n_j}{l_j} \right) \lambda^{\|\mathbf{l}\|_1} (1-\lambda)^{N-\|\mathbf{l}\|_1} \, |\mathbf{l}\rangle\langle\mathbf{l}| \, , \tag{S183}$$

where the inequality between vectors $\mathbf{a} \ge \mathbf{b}$ means that $a_j \ge b_j$ for all $j = 1, \ldots, K$. Consequently, by using that $\sum_{P=0}^{\infty} \Pi_P^{(K)} = \mathbb{1}$, it holds that

$$\begin{aligned} \mathscr{P}_F &:= \mathrm{Tr}\left[\Phi_{g,0}^{\otimes K}\left(\mathscr{E}_{\lambda,0}^{\otimes K}(|\mathbf{n}\rangle\langle\mathbf{n}|)\right) \Pi_F^{(K)}\right] = \sum_{P,P'=0}^{\infty} \mathrm{Tr}\left[\Phi_{g,0}^{\otimes K}\left(\Pi_P^{(K)} \mathscr{E}_{\lambda,0}^{\otimes K}(|\mathbf{n}\rangle\langle\mathbf{n}|) \Pi_{P'}^{(K)}\right) \Pi_F^{(K)}\right] \\ &= \sum_{P=0}^{N} \lambda^P (1-\lambda)^{N-P} \sum_{\substack{\mathbf{l}\in\mathbb{N}^K \\ \mathbf{l}\le\mathbf{n} \\ \|\mathbf{l}\|_1 = P}} \left(\prod_{j=1}^{K} \binom{n_j}{l_j} \right) \mathrm{Tr}\left[\Phi_{g,0}^{\otimes K}\left(|\mathbf{l}\rangle\langle\mathbf{l}|\right) \Pi_F^{(K)}\right] . \end{aligned} \tag{S184}$$

Moreover, (S99) implies that for all $l \in \mathbb{N}$ it holds that

$$\Phi_{g,0}(|l\rangle\langle l|) = \frac{1}{g^{l+1}} \sum_{m=0}^{\infty} \binom{l+m}{l} \left(\frac{g-1}{g}\right)^m |m+l\rangle\langle m+l| \tag{S185}$$

and hence

$$\Phi_{g,0}^{\otimes K}(|\mathbf{l}\rangle\langle\mathbf{l}|) = \frac{1}{g^{P+K}} \sum_{\mathbf{m}\in\mathbb{N}^K} \left(\prod_{j=1}^{K} \binom{l_j+m_j}{l_j} \right) \left(\frac{g-1}{g}\right)^{\|\mathbf{m}\|_1} |\mathbf{m}+\mathbf{l}\rangle\langle\mathbf{m}+\mathbf{l}| \, . \tag{S186}$$

Consequently, it holds that

$$\mathrm{Tr}\left[\Phi_{g,0}^{\otimes K}\left(|\mathbf{l}\rangle\langle\mathbf{l}|\right) \Pi_F^{(K)}\right] = \frac{(g-1)^{F-P}}{g^{K+F}} \sum_{\substack{\mathbf{m}\in\mathbb{N}^K \\ \|\mathbf{m}\|_1 = F-P}} \prod_{j=1}^{K} \binom{l_j+m_j}{l_j} . \tag{S187}$$

The sum

$$\sum_{\substack{\mathbf{m}\in\mathbb{N}^K \\ \|\mathbf{m}\|_1 = F-P}} \prod_{j=1}^{K} \binom{l_j+m_j}{l_j} , \tag{S188}$$

which appears in (S187), is the coefficient of the term x^{F-P} of the power series $Q(x)$ in the variable $x \in (0,1)$ defined as

$$Q(x) := \sum_{\mathbf{m}\in\mathbb{N}^K} \left(\prod_{j=1}^{K} \binom{l_j+m_j}{l_j} \right) x^{\|\mathbf{m}\|_1} . \tag{S189}$$

By exploiting that for all $l \in \mathbb{N}$ it holds that

$$\sum_{m=0}^{\infty} \binom{m+l}{m} x^m = \frac{1}{(1-x)^{l+1}} , \tag{S190}$$

one obtains that

$$Q(x)=\sum_{\mathbf{m}\in\mathbb{N}^K}\left(\prod_{j=1}^K\binom{l_j+m_j}{l_j}\right)x^{\|\mathbf{m}\|_1}=\prod_{j=1}^K\left(\sum_{m=0}^\infty\binom{l_j+m}{m}x^m\right)=\prod_{j=1}^K\frac{1}{(1-x)^{l_j+1}}=\frac{1}{(1-x)^{P+K}}$$
$$=\sum_{m=0}^\infty\binom{P+K+m-1}{m}x^m\,. \tag{S191}$$

It follows that

$$\sum_{\substack{\mathbf{m}\in\mathbb{N}^K\\ \|\mathbf{m}\|_1=F-P}}\prod_{j=1}^K\binom{l_j+m_j}{l_j}=\binom{K+F-1}{F-P}\Theta(F-P) \tag{S192}$$

and hence

$$\mathrm{Tr}\left[\Phi_{g,0}^{\otimes K}\left(|\mathbf{l}\rangle\!\langle\mathbf{l}|\right)\Pi_F^{(K)}\right]=\frac{(g-1)^{F-P}}{g^{K+F}}\binom{K+F-1}{F-P}\Theta(F-P)\,, \tag{S193}$$

where we have introduced the Heaviside function $\Theta(x)$ defined as $\Theta(x)=1$ if $x\geq 0$, and $\Theta(x)=0$ if $x<0$. Consequently, (S184) implies that

$$\mathscr{P}_F=\sum_{P=0}^{\min(F,N)}\lambda^P(1-\lambda)^{N-P}\frac{(g-1)^{F-P}}{g^{K+F}}\binom{K+F-1}{F-P}\sum_{\substack{\mathbf{l}\in\mathbb{N}^K\\ \mathbf{l}\leq\mathbf{n}\\ \|\mathbf{l}\|_1=P}}\left(\prod_{j=1}^K\binom{n_j}{l_j}\right)$$
$$=\sum_{P=0}^{\min(F,N)}\binom{N}{P}\lambda^P(1-\lambda)^{N-P}\frac{(g-1)^{F-P}}{g^{K+F}}\binom{K+F-1}{F-P}\,, \tag{S194}$$

where in the last equality we have exploited that

$$\sum_{\substack{\mathbf{l}\in\mathbb{N}^K\\ \mathbf{l}\leq\mathbf{n}\\ \|\mathbf{l}\|_1=P}}\left(\prod_{j=1}^K\binom{n_j}{l_j}\right)=\binom{N}{P}. \tag{S195}$$

This follows from the fact that the sum in (S195) is equal to the coefficient of the term x^P of the following polynomial in the variable $x\in\mathbb{R}$:

$$\sum_{\substack{\mathbf{l}\in\mathbb{N}^K\\ \mathbf{l}\leq\mathbf{n}}}\left(\prod_{j=1}^K\binom{n_j}{l_j}\right)x^{\|\mathbf{l}\|_1}=\prod_{j=1}^K(1+x)^{n_j}=(1+x)^N=\sum_{l=0}^N\binom{N}{l}x^l\,. \tag{S196}$$

□

Remark 3. *Here we present an alternative method to calculate the probability* $\mathscr{P}_F$ *reported in* (S179). *For all* $x\in(0,1)$ *let us consider the tensor product of* K *thermal states with mean photon number* $\frac{x}{1-x}$, *i.e.*

$$\tau_{\frac{x}{1-x}}^{\otimes K}=(1-x)^K\sum_{\boldsymbol{l}\in\mathbb{N}^K}x^{\|\boldsymbol{l}\|_1}\,|\boldsymbol{l}\rangle\!\langle\boldsymbol{l}|\,. \tag{S197}$$

Consequently, the quantity

$$\mathscr{P}_F=\mathrm{Tr}\left[\mathcal{N}_{g,\lambda}^{\otimes K}(|\boldsymbol{n}\rangle\!\langle\boldsymbol{n}|)\,\Pi_F^{(K)}\right] \tag{S198}$$

is the coefficient of the term x^F *of the power series* $P(x)$ *in the variable* $x\in(0,1)$ *defined as*

$$P(x):=\frac{1}{(1-x)^K}\,\mathrm{Tr}\left[\mathcal{N}_{g,\lambda}^{\otimes K}(|\boldsymbol{n}\rangle\!\langle\boldsymbol{n}|)\,\tau_{\frac{x}{1-x}}^{\otimes K}\right]\,. \tag{S199}$$

By using the characteristic function properties reported in (S2), (S3), (S72), *and the fact that the characteristic function of a thermal state* τ_ν *is* $\chi_{\tau_\nu}(\mathbf{r}) = e^{-\frac{1}{4}(2\nu+1)|\mathbf{r}|^2}$, *one obtains that for any single-mode state* ρ *it holds that*

$$\begin{aligned} \mathrm{Tr}\left[\mathscr{N}_{g,\lambda}(\rho)\,\tau_{\frac{x}{1-x}}\right] &= \int_{\mathbb{R}^2}\frac{\mathrm{d}^2\mathbf{r}}{2\pi}\chi_{\mathscr{N}_{g,\lambda}(\rho)}(\mathbf{r})\,\chi_{\tau_{\frac{x}{1-x}}}(\mathbf{r}) = \int_{\mathbb{R}^2}\frac{\mathrm{d}^2\mathbf{r}}{2\pi}\chi_\rho(\sqrt{g\lambda}\,\mathbf{r})e^{-\frac{1}{4}\left(2g-g\lambda+2\frac{x}{1-x}\right)|\mathbf{r}|^2} \\ &= \frac{1}{g\lambda}\int_{\mathbb{R}^2}\frac{\mathrm{d}^2\mathbf{r}}{2\pi}\chi_\rho(\mathbf{r})e^{-\frac{1}{4g\lambda}\left(2g-g\lambda+2\frac{x}{1-x}\right)|\mathbf{r}|^2} = \frac{1}{g\lambda}\,\mathrm{Tr}\left[\rho\;\tau_{\frac{g-g\lambda+(1+g\lambda-g)x}{g\lambda(1-x)}}\right]. \end{aligned} \tag{S200}$$

Hence, by exploiting (S190) *and the fact that* $\|\boldsymbol{n}\|_1 = N$, *the power series* $P(x)$ *can be expressed as*

$$\begin{aligned} P(x) &= \frac{1}{(1-x)^K(g\lambda)^K}\,\mathrm{Tr}\left[|\boldsymbol{n}\rangle\!\langle\boldsymbol{n}|\,\tau^{\otimes K}_{\frac{g-g\lambda+(1+g\lambda-g)x}{g\lambda(1-x)}}\right] = \frac{[g(1-\lambda)+(1+g\lambda-g)x]^N}{[g-(g-1)x]^{N+K}} \\ &= \sum_{P=0}^{N}\binom{N}{P}(1+g\lambda-g)^P(1-\lambda)^{N-P}g^{-P-K}x^P\sum_{l=0}^{\infty}\binom{N+K-1+l}{l}\left(\frac{g-1}{g}\right)^l x^l\,. \end{aligned} \tag{S201}$$

It follows that

$$\mathscr{P}_F = \sum_{P=0}^{\min(F,N)}\binom{N}{P}\binom{N+K+F-P-1}{F-P}(1+g\lambda-g)^P(1-\lambda)^{N-P}\frac{(g-1)^{F-P}}{g^{F+K}}\,. \tag{S202}$$

Incidentally, by comparing the two expressions of $\mathscr{P}_F$ *in* (S179) *and* (S202), *one deduces the following identity:*

$$\sum_{P=0}^{\min(F,N)}\binom{N}{P}\binom{K+F-1+N-P}{F-P}\left(\frac{g\lambda-(g-1)}{(1-\lambda)(g-1)}\right)^P = \sum_{P=0}^{\min(F,N)}\binom{N}{P}\binom{K+F-1}{F-P}\left(\frac{\lambda}{(1-\lambda)(g-1)}\right)^P\,. \tag{S203}$$

Let us now introduce an additional entanglement distribution protocol to distribute ebits across any piBGC $\mathscr{N}_{g,\lambda}$. The protocol depends on two parameters, $K, N \in \mathbb{N}^+$ with $K \ge 2$, and it is composed of five steps named S1-S5, which we now outline.

S1: Alice prepares the state $|\Psi_{N,K}\rangle_{A_1\ldots A_K,A'_1,\ldots,A'_K}$ of $K+K$ modes $A_1,\ldots,A_k,A'_1,\ldots,A'_K$, sending the systems $A'_1,\ldots,A'_K$ to Bob through K uses of the channel $\mathscr{N}_{g,\lambda}$. Now Alice and Bob share the state $\mathrm{Id}_{A_1\ldots A_k}\otimes\mathscr{N}_{g,\lambda}^{\otimes K}(|\Psi_{N,K}\rangle\!\langle\Psi_{N,K}|)$. By using (S78), such a state can be expressed as

$$\begin{aligned} &\mathrm{Id}_{A_1\ldots A_k}\otimes\mathscr{N}_{g,\lambda}^{\otimes K}(|\Psi_{N,K}\rangle\!\langle\Psi_{N,K}|) \\ &= \frac{1}{\binom{N+K-1}{N}}\sum_{\substack{\mathbf{n}\in\mathbb{N}^K\\ \|\mathbf{n}\|_1=N}}\;\sum_{\substack{\mathbf{i}\in\mathbb{N}^K\\ \|\mathbf{i}\|_1=N}}\;\sum_{\substack{\mathbf{l}\in\mathbb{N}^K\\ \mathbf{l}\ge\max(\mathbf{i}-\mathbf{n},\mathbf{0})}}\left(\prod_{j=1}^{K}f_{n_j,i_j,l_j}(g,\lambda)\right)|\mathbf{n}\rangle\!\langle\mathbf{i}|_{A_1\ldots A_K}\otimes|\mathbf{l}+\mathbf{n}-\mathbf{i}\rangle\!\langle\mathbf{l}|_{B_1\ldots B_K}\,, \end{aligned} \tag{S204}$$

where $\mathbf{0}\in\mathbb{N}^K$ is the zero vector and the inequality between vectors $\mathbf{a}\ge\mathbf{b}$ means that $a_j \ge b_j$ for all $j = 1,\ldots,K$.

S2: Bob performs the local POVM $\{\Pi_F^{(K)}\}_{F\in\mathbb{N}}$, where $\Pi_F^{(K)}$ is the projector onto the subspace whose total photon number equals F (see (S178)), on the K modes he has received. The probability of getting the outcome F is denoted by $\mathscr{P}_F$ and it can be calculated as

$$\begin{aligned} \mathscr{P}_F &:= \mathrm{Tr}\left[\left(\mathbb{1}_{A_1\ldots A_k}\otimes\Pi_F^{(K)}\right)\left(\mathrm{Id}_{A_1\ldots A_k}\otimes\mathscr{N}_{g,\lambda}^{\otimes K}(|\Psi_{N,K}\rangle\!\langle\Psi_{N,K}|)\right)\right] = \frac{1}{\binom{N+K-1}{N}}\sum_{\substack{\mathbf{n}\in\mathbb{N}^K\\ \|\mathbf{n}\|_1=N}}\mathrm{Tr}\left[\Pi_F^{(K)}\,\mathscr{N}_{g,\lambda}^{\otimes K}(|\mathbf{n}\rangle\!\langle\mathbf{n}|)\right] \\ &= \sum_{P=0}^{\min(F,N)}\binom{N}{P}\binom{K+F-1}{F-P}\lambda^P(1-\lambda)^{N-P}\frac{(g-1)^{F-P}}{g^{K+F}}\,, \end{aligned} \tag{S205}$$

where we have exploited Lemma S16. The post-measurement state $\rho^{(F)}_{A_1\ldots A_k B_1\ldots B_k}$ conditioned on the outcome $F\in\mathbb{N}$ is given by

$$\begin{aligned}
&\rho^{(F)}_{A_1\ldots A_k B_1\ldots B_k}\\
&\quad= \frac{1}{\mathscr{P}_F}\left(\mathbb{1}_{A_1\ldots A_k}\otimes \Pi^{(K)}_F\right)\left(\mathrm{Id}_{A_1\ldots A_k}\otimes \mathscr{N}^{\otimes K}_{g,\lambda}(|\Psi_{N,K}\rangle\!\langle\Psi_{N,K}|)\right)\left(\mathbb{1}_{A_1\ldots A_k}\otimes \Pi^{(K)}_F\right)\\
&\quad= \frac{1}{\mathscr{P}_F\binom{N+K-1}{N}}\sum_{\substack{\mathbf{n}\in\mathbb{N}^K\\ \|\mathbf{n}\|_1=N}}\sum_{\substack{\mathbf{i}\in\mathbb{N}^K\\ \|\mathbf{i}\|_1=N}}\sum_{\substack{\mathbf{l}\in\mathbb{N}^K\\ \|\mathbf{l}\|_1=F\\ \mathbf{l}\geq\max(\mathbf{i}-\mathbf{n},\mathbf{0})}}\left(\prod_{j=1}^K f_{n_j,i_j,l_j}(g,\lambda)\right)|\mathbf{n}\rangle\!\langle\mathbf{i}|_{A_1\ldots A_K}\otimes|\mathbf{l}+\mathbf{n}-\mathbf{i}\rangle\!\langle\mathbf{l}|_{B_1\ldots B_K}\\
&\quad= \sum_{n,i=0}^{\binom{N+K-1}{N}-1}\ \sum_{h,l=0}^{\binom{F+K-1}{F}-1} c_{n,i,h,l}\,|\phi^{(N)}_n\rangle\!\langle\phi^{(N)}_i|_{A_1\ldots A_k}\otimes|\phi^{(F)}_h\rangle\!\langle\phi^{(F)}_l|_{B_1\ldots B_k}\,,
\end{aligned} \tag{S206}$$

where for all $n,i=0,1,\ldots,\binom{N+K-1}{N}-1$ and all $h,l=0,1,\ldots,\binom{F+K-1}{F}-1$ the coefficient $c_{n,i,h,l}$ is defined as follows. Let $\mathbf{n},\mathbf{i},\mathbf{h},\mathbf{l}\in\mathbb{N}^K$ such that $|\phi^{(N)}_n\rangle=|\mathbf{n}\rangle$, $|\phi^{(N)}_i\rangle=|\mathbf{i}\rangle$, $|\phi^{(F)}_h\rangle=|\mathbf{h}\rangle$, and $|\phi^{(F)}_l\rangle=|\mathbf{l}\rangle$. If $\mathbf{l}\geq\max(\mathbf{i}-\mathbf{n},\mathbf{0})$ and $\mathbf{h}=\mathbf{l}+\mathbf{n}-\mathbf{i}$, then

$$c_{n,i,h,l}\coloneqq\frac{\left(\prod_{j=1}^K f_{n_j,i_j,l_j}(g,\lambda)\right)}{\mathscr{P}_F\binom{N+K-1}{N}}\,, \tag{S207}$$

otherwise $c_{n,i,h,l}=0$. By setting

$$d\coloneqq\max\left(\binom{N+K-1}{N},\binom{F+K-1}{F}\right)\,, \tag{S208}$$

the resulting state in (S206) can be seen as a bipartite two-qu$d$it state $\rho^{(F)}_{AB}\in\mathfrak{S}(\mathcal{H}_d\otimes\mathcal{H}_d)$ of the form

$$\rho^{(F)}_{AB}=\sum_{n,i,h,l=0}^{d-1}\eta_{n,i,h,l}\,|n\rangle\!\langle i|_A\otimes|h\rangle\!\langle l|_B\,, \tag{S209}$$

where $\mathcal{H}_d$ is the qu$d$it Hilbert space with $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle\}$ as an orthonormal basis, and where the coefficients $\eta_{n,i,h,l}$ are defined as follows:

- if $n,i\leq\binom{N+K-1}{N}-1$ and $h,l\leq\binom{F+K-1}{F}-1$, then $\eta_{n,i,h,l}\coloneqq c_{n,i,h,l}$;
- otherwise, $\eta_{n,i,h,l}\coloneqq 0$.

Consequently, Alice and Bob have reduced the problem in distilling ebits from the two-qu$d$it state $\rho^{(F)}_{AB}$.

S3: Now Alice and Bob decide whether or not to run the reverse hashing protocol, which can distil ebits from $\rho^{(F)}_{AB}$ with a rate equal to its reverse coherent information, i.e.

$$I_{\mathrm{rc}}(\rho^{(F)}_{AB})=S(\mathrm{Tr}_B\,\rho^{(F)}_{AB})-S(\rho^{(F)}_{AB})\,, \tag{S210}$$

where $S(\cdot)$ denotes the von Neumann entropy. By exploiting that

$$\mathrm{Tr}_B\,\rho^{(F)}_{AB}=\frac{1}{\binom{N+K-1}{N}}\sum_{n=0}^{\binom{N+K-1}{N}-1}|n\rangle\!\langle n|\,, \tag{S211}$$

as guaranteed by (S206) and Lemma S16, it follows that the reverse coherent information can be calculated as

$$I_{\mathrm{rc}}(\rho^{(F)}_{AB})=\log_2\binom{N+K-1}{N}-S\left(\sum_{n,i,h,l=0}^{d-1}\eta_{n,i,h,l}\,|n\rangle\!\langle i|\otimes|h\rangle\!\langle l|\right)\,. \tag{S212}$$

If Alice and Bob choose to run the reverse hashing protocol, the protocol terminates. Otherwise, they apply the qu$d$it Pauli-based twirling reported in [16, Eq. (18)] in order to transform their state in a Bell-diagonal state of the form

$$\rho_{AB}^{\prime(F)} = \sum_{m,n=0}^{d} \alpha_{mn}^{(F,0)} |\psi_{mn}^{(d)}\rangle\langle\psi_{mn}^{(d)}|_{AB} \,, \tag{S213}$$

where

$$|\psi_{mn}^{(d)}\rangle_{AB} := \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} e^{i\frac{2\pi m r}{d}} |r\rangle_A \otimes |(r-n) \bmod d\rangle_B \tag{S214}$$

and

$$\alpha_{mn}^{(F,0)} := \langle\psi_{mn}^{(d)}|\, \rho_{AB}^{(F)}\, |\psi_{mn}^{(d)}\rangle = \frac{1}{d} \sum_{r_1,r_2=0}^{d-1} \cos\left(\frac{2\pi m(r_2-r_1)}{d}\right) \eta_{r_1,r_2,\,(r_1-n) \bmod d,\,(r_2-n) \bmod d} \,. \tag{S215}$$

S4: Alice and Bob run $\bar{k}$ times the P1-or-P2 sub-routine for qu$d$its [16], where $\bar{k}$ is chosen in order to maximise the ebit rate. The goal of this step is to bring the shared state closer to the d-dimensional maximally-entangled state $|\psi_{00}^{(d)}\rangle$. This step is successful, i.e. the protocol is not aborted, with a probability of success equal to $\prod_{t=0}^{\bar{k}-1} P_t^{(F)}$ and it allows Alice and Bob to transform $2^{\bar{k}}$ copies of $\rho_{AB}^{\prime(F)} = \sum_{m,n=0}^{d} \alpha_{mn}^{(F,0)} |\psi_{mn}^{(d)}\rangle\langle\psi_{mn}^{(d)}|_{AB}$ in a state of the form

$$\rho_{AB}^{\prime(F,\bar{k})} := \sum_{m,n=0}^{d} \alpha_{mn}^{(F,\bar{k})} |\psi_{mn}^{(d)}\rangle\langle\psi_{mn}^{(d)}|_{AB} \,. \tag{S216}$$

For all $t \in \{0,1,\ldots,\bar{k}-1\}$ and all $m,n \in \{0,1,\ldots,d-1\}$ the coefficients $\alpha_{mn}^{(F,t+1)}$ and the probabilities $P_t^{(F)}$ are recursively defined in the following way [16]:

- If $\sum_{m_1=0}^{d-1} \alpha_{m_1 0}^{(F,t)} < \sum_{n_1=0}^{d-1} \alpha_{0 n_1}^{(F,t)}$, then

$$\alpha_{mn}^{(F,t+1)} := \frac{1}{P_t^{(F)}} \sum_{\substack{m_1,m_2=0 \\ (m_1+m_2) \bmod d = m}}^{d-1} \alpha_{m_1 n}^{(F,t)} \alpha_{m_2 n}^{(F,t)} \,, \tag{S217}$$

  where

$$P_t^{(F)} := \sum_{m_1,m_2,n=0}^{d-1} \alpha_{m_1 n}^{(F,t)} \alpha_{m_2 n}^{(F,t)} \,. \tag{S218}$$

- Otherwise,

$$\alpha_{mn}^{(F,t+1)} := \frac{1}{P_t^{(F)}} \sum_{\substack{n_1,n_2=0 \\ (n_1+n_2) \bmod d = n}}^{d-1} \alpha_{m n_1}^{(F,t)} \alpha_{m n_2}^{(F,t)} \,, \tag{S219}$$

  where

$$P_t^{(F)} := \sum_{m,n_1,n_2=0}^{d-1} \alpha_{m n_1}^{(F,t)} \alpha_{m n_2}^{(F,t)} \,. \tag{S220}$$

S5: Alice and Bob distil ebits from the state $\rho_{AB}^{\prime(F,\bar{k})} = \sum_{m,n=0}^{d} \alpha_{mn}^{(F,\bar{k})} |\psi_{mn}^{(d)}\rangle\langle\psi_{mn}^{(d)}|_{AB}$ with a yield denoted as $\mathscr{I}_d(\alpha^{(F,\bar{k})})$ by running the following protocol:

- If $d=2$, then Alice and Bob run the Step 5 and Step 6 of the entanglement distribution protocol introduced in the proof of Theorem S13 in order to distil ebits from $\rho'^{(F,\bar{k})}_{AB}$ with a yield equal to

$$\mathscr{I}_2(\alpha^{(F,\bar{k})}) := \mathscr{I}(\alpha^{(F,\bar{k})}_{00}, \alpha^{(F,\bar{k})}_{01}, \alpha^{(F,\bar{k})}_{10}, \alpha^{(F,\bar{k})}_{11}) , \tag{S221}$$

where $\mathscr{I}$ is defined in (S130).

- If $d>2$, then Alice and Bob run the hashing protocol on $\rho'^{(F,\bar{k})}_{AB}$ and thus they distil ebits with a yield equal to the coherent information of $\rho'^{(F,\bar{k})}_{AB}$, i.e.

$$\mathscr{I}_d(\alpha^{(F,\bar{k})}) := I_{\mathrm{c}}(\rho'^{(F,\bar{k})}_{AB}) = \log_2 d + \sum_{m,n=0}^{d-1} \alpha^{(F,\bar{k})}_{mn} \log_2 \alpha^{(F,\bar{k})}_{mn} . \tag{S222}$$

The ebit rate of the protocol is given by

$$R(g,\lambda,N,K) := \frac{1}{K}\sum_{F=1}^{\infty} \mathscr{P}_F \max\left(I_{\mathrm{rc}}(\rho^{(F)}_{AB}) , \sup_{\bar{k}\in\mathbb{N}} \frac{\prod_{t=0}^{\bar{k}-1} P_t^{(F)}}{2^{\bar{k}}} \mathscr{I}_d(\alpha^{(F,\bar{k})}) \right) . \tag{S223}$$

The term $\frac{1}{K}$ in the expression (S223) arises from the fact that Alice uses the channel K times during step S1, and the variable F corresponds to the outcome of the total photon number measurement in step S2, with associated probability $\mathscr{P}_F$. The sum over F equals the expected value of the yield of ebits that can be distilled from the post-measurement state $\rho^{(F)}_{AB}$ by running steps S3, S4, and S5. The maximum comes from the fact that during step S3 Alice and Bob choose whether or not to run the reverse hashing protocol, which can distil ebits with a rate equal to $I_{\mathrm{rc}}(\rho^{(F)}_{AB})$. The supremum over $\bar{k}$ comes from the fact that Alice and Bob choose the number of iterations $\bar{k}$ of the P1-or-P2 subroutine in order to maximise the rate. The rate in (S223) is a lower bound on the two-way quantum capacity of the piBGC $\mathscr{N}_{g,\lambda}$ for all $N,K\in\mathbb{N}^+$ with $K\geq 2$. Therefore, we have

$$K(\mathscr{N}_{g,\lambda}) \geq Q_2(\mathscr{N}_{g,\lambda}) \geq \sup_{\substack{N,K\in\mathbb{N}^+\\ K\geq 2}} R(g,\lambda,N,K) . \tag{S224}$$

Let us summarise this result in the following theorem.

Theorem S17. *For all $\lambda\in[0,1]$ and $g\geq 1$ the secret-key capacity $K(\mathscr{N}_{g,\lambda})$ and the two-way quantum capacity $Q_2(\mathscr{N}_{g,\lambda})$ of the piBGC $\mathscr{N}_{g,\lambda}$ satisfy*

$$K(\mathscr{N}_{g,\lambda}) \geq Q_2(\mathscr{N}_{g,\lambda}) \geq \sup_{\substack{N,K\in\mathbb{N}^+\\ K\geq 2}} R(g,\lambda,N,K) , \tag{S225}$$

where

$$R(g,\lambda,N,K) := \frac{1}{K}\sum_{F=1}^{\infty} \mathscr{P}_F \max\left(I^{(F)}_{rc} , \sup_{\bar{k}\in\mathbb{N}} \frac{\prod_{t=0}^{\bar{k}-1} P_t^{(F)}}{2^{\bar{k}}} \mathscr{I}_d(\alpha^{(F,\bar{k})}) \right) . \tag{S226}$$

The quantities present in (S226) *are defined as follows. For all $F\in\mathbb{N}$ the dimension d is defined as*

$$d := \max\left(\binom{N+K-1}{N}, \binom{F+K-1}{F} \right) \tag{S227}$$

and the probability $\mathscr{P}_F$ is defined as

$$\mathscr{P}_F := \sum_{P=0}^{\min(F,N)} \binom{N}{P}\binom{K+F-1}{F-P} \lambda^P (1-\lambda)^{N-P} \frac{(g-1)^{F-P}}{g^{K+F}} . \tag{S228}$$

Moreover, the probabilities $P^{(F)}_{\bar{k}}$ and the coefficients $\{\alpha^{(F,\bar{k})}_{mn}\}_{m,n\in\{0,1,\ldots,d-1\}}$ are recursively defined as follows. For all $t\in\{0,1,\ldots,\bar{k}-1\}$ and all $m,n\in\{0,1,\ldots,d-1\}$ it holds that:

- *If* $\sum_{m_1=0}^{d-1} \alpha_{m_1 0}^{(F,t)} < \sum_{n_1=0}^{d-1} \alpha_{0 n_1}^{(F,t)}$, *then*

$$\begin{aligned} \alpha_{mn}^{(F,t+1)} &:= \frac{1}{P_t^{(F)}} \sum_{\substack{m_1,m_2=0 \\ (m_1+m_2) \bmod d=m}}^{d-1} \alpha_{m_1 n}^{(F,t)} \alpha_{m_2 n}^{(F,t)} \,, \\ P_t^{(F)} &:= \sum_{m_1,m_2,n=0}^{d-1} \alpha_{m_1 n}^{(F,t)} \alpha_{m_2 n}^{(F,t)} \,. \end{aligned} \tag{S229}$$

- *Otherwise,*

$$\begin{aligned} \alpha_{mn}^{(F,t+1)} &:= \frac{1}{P_t^{(F)}} \sum_{\substack{n_1,n_2=0 \\ (n_1+n_2) \bmod d=n}}^{d-1} \alpha_{m n_1}^{(F,t)} \alpha_{m n_2}^{(F,t)} \,, \\ P_t^{(F)} &:= \sum_{m,n_1,n_2=0}^{d-1} \alpha_{m n_1}^{(F,t)} \alpha_{m n_2}^{(F,t)} \,. \end{aligned} \tag{S230}$$

Moreover, for all $m, n \in \{0, 1, \ldots, d-1\}$ *the coefficient* $\alpha_{mn}^{(F,0)}$ *is defined as*

$$\alpha_{mn}^{(F,0)} := \frac{1}{d} \sum_{r_1,r_2=0}^{d-1} \cos\left(\frac{2\pi m(r_2-r_1)}{d}\right) \eta_{r_1,r_2,(r_1-n) \bmod d,(r_2-n) \bmod d} \,. \tag{S231}$$

In addition, for all $n, i \in 0, 1, \ldots, \binom{N+K-1}{N} - 1$, *we define* $(n_1, \ldots, n_K)$ *and* $(i_1, \ldots, i_K)$ *as the* n*th and* i*th element of the ordered set* $S_{K,N}$, *where* $S_{K,N}$ *is defined as*

$$S_{K,N} := \{(f_1, \ldots, f_K) \in \mathbb{N}^K : \sum_{j=1}^{K} f_j = N\} \tag{S232}$$

and it is ordered according to the relation $\preceq_{K,N}$, *given by*

$$(f_1, \ldots, f_K) \preceq_{K,N} (g_1, \ldots, g_K) \iff \sum_{j=1}^{K} f_j \,(N+1)^j < \sum_{j=1}^{K} g_j \,(N+1)^j \,. \tag{S233}$$

Additionally, for all $h, l \in \{0, 1, \ldots, \binom{F+K-1}{F} - 1\}$, *we define* $(h_1, \ldots, h_K)$ *and* $(l_1, \ldots, l_K)$ *as the* h*th and* l*th element of the set* $S_{K,F}$ *ordered according to the relation* $\preceq_{F,N}$. *Furthermore, for all* $n, i, h, l \in \{0, 1, \ldots, d-1\}$ *the coefficients* $\eta_{n,i,h,l}$ *are defined as follows:*

- *If*

$$\begin{aligned} n, i &\leq \binom{N+K-1}{N} - 1 \,, \\ h, l &\leq \binom{F+K-1}{F} - 1 \,, \\ l_j &\geq \max(i_j - n_j, 0) \quad \textit{for all } j = 1, 2, \ldots, K \,, \\ h_j &= l_j + n_j - i_j \quad \textit{for all } j = 1, 2, \ldots, K \,, \end{aligned} \tag{S234}$$

then

$$\eta_{n,i,h,l} := \frac{\left(\prod_{j=1}^{K} f_{n_j,i_j,l_j}(g,\lambda)\right)}{\mathscr{P}_F \binom{N+K-1}{N}} \,, \tag{S235}$$

where $f_{n,i,l}(g, \lambda)$ *is defined in* (S79).

- *Otherwise,* $\eta_{n,i,h,l} = 0$.

Moreover, the quantity $I_{rc}^{(F)}$ *is defined as*

$$I_{rc}^{(F)} := \log_2 \binom{N+K-1}{N} - S\left(\sum_{n,i,h,l=0}^{d-1} \eta_{n,i,h,l}\, |n\rangle\langle i| \otimes |h\rangle\langle l|\right), \tag{S236}$$

where $S(\cdot)$ *denotes the von Neumann entropy. Finally, the term* $\mathscr{I}_d(\alpha^{(F,\bar{k})})$ *is defined differently depending on the value of* d*:*

- *If* $d = 2$*, then*

$$\mathscr{I}_2(\alpha^{(F,\bar{k})}) := \mathscr{I}(\alpha_{00}^{(F,\bar{k})}, \alpha_{01}^{(F,\bar{k})}, \alpha_{10}^{(F,\bar{k})}, \alpha_{11}^{(F,\bar{k})}), \tag{S237}$$

  where $\mathscr{I}$ *is defined in* (S130).

- *If* $d > 2$*, then*

$$\mathscr{I}_d(\alpha^{(F,\bar{k})}) := \log_2 d + \sum_{m,n=0}^{d-1} \alpha_{mn}^{(F,\bar{k})} \log_2 \alpha_{mn}^{(F,\bar{k})}. \tag{S238}$$

V. RESULTS ON THE TWO-WAY CAPACITIES OF PIBGCS

In this subsection, for each of the piBGCs, first we determine the parameter region where the two-way capacities vanish, second we find a new lower bound on the two-way capacities, and finally we compare our results with the existing literature.

A. Results on the two-way capacities of the thermal attenuator

Let us consider the thermal attenuator $\mathscr{E}_{\lambda,\nu}$ of transmissivity $\lambda \in [0,1]$ and thermal noise $\nu \geq 0$. Since the PLOB bound in (S32) vanishes for $\lambda \leq \frac{\nu}{\nu+1}$, it is already known that the two-way capacities of $\mathscr{E}_{\lambda,\nu}$ vanish for $\lambda < \frac{\nu}{\nu+1}$. The following theorem establishes that also the vice-versa is true.

Theorem S18. *Let* $\lambda \in [0,1]$*,* $\nu \geq 0$*, and* $N_s > 0$*. The energy-constrained two-way capacities of the thermal attenuator* $Q_2(\mathscr{E}_{\lambda,\nu}, N_s)$ *and* $K(\mathscr{E}_{\lambda,\nu}, N_s)$ *vanish if and only if* $\lambda \leq \frac{\nu}{\nu+1}$*, i.e. if and only if* $\mathscr{E}_{\lambda,\nu}$ *is entanglement breaking. In particular, the same holds for the unconstrained two-way capacities.*

Proof. Theorem S18 is a direct consequence of Lemma S4 and Theorem S12. □

The validity of Theorem S18 was not known before the present work. Indeed, in [30, 62] the authors says that it is an open problem to determine the exact value of the maximum tolerable excess noise, which is defined by

$$\epsilon(\lambda) := \frac{1-\lambda}{\lambda} \max\{\nu \geq 0 \,:\, K(\mathscr{E}_{\lambda,\nu}) > 0\}. \tag{S239}$$

Theorem S12 implies that $\varepsilon(\lambda) = 1$ for all $\lambda \in (0,1)$. Hence, we have answered to the question, which was deemed "crucial" in [30, Section 7], "What is the maximum excess noise that is tolerable in QKD? I.e., optimizing over all QKD protocols?" In [30, 62] the authors showed, by applying the PLOB bound, the upper bound $\varepsilon(\lambda) \leq 1$ and provided also a lower bound on $\varepsilon(\lambda)$ which was far from 1.

Except for the special case $\nu = 0$, it is an open question whether the reverse coherent information lower bound in Eq. S34 equals the true two-way quantum capacity of the thermal attenuator $Q_2(\mathscr{E}_{\lambda,\nu})$: Theorem S18 provides a negative answer to this question. Indeed, although $Q_2(\mathscr{E}_{\lambda,\nu}) = 0$ if and only if $\lambda \leq \frac{\nu}{\nu+1}$ (thanks to Theorem S18), the reverse coherent information lower bound vanishes for all $\lambda \leq 1 - 2^{-h(\nu)}$. Hence, since $1 - 2^{-h(\nu)} > \frac{\nu}{\nu+1}$ for all $\nu > 0$, the reverse coherent information lower bound is not equal to $Q_2(\mathscr{E}_{\lambda,\nu})$ at least in the region $\nu > 0$ and $\lambda \in (\frac{\nu}{\nu+1}, 1 - 2^{-h(\nu)}]$. In the following theorem we obtain an improved lower bound on the two-way capacities of the thermal attenuator.

Theorem S19. *Let $\lambda \in [0,1]$, $\nu \geq 0$, and $N_s \geq 0$. The EC two-way capacities $Q_2(\mathscr{E}_{\lambda,\nu}, N_s)$ and $K(\mathscr{E}_{\lambda,\nu}, N_s)$ of the thermal attenuator $\mathscr{E}_{\lambda,\nu}$ satisfy the following lower bound*

$$K(\mathscr{E}_{\lambda,\nu}, N_s) \geq Q_2(\mathscr{E}_{\lambda,\nu}, N_s) \geq \sup_{\substack{c\in(0,1),\, M\in\mathbb{N}^+,\, k\in\mathbb{N} \\ (1-c^2)M\leq N_s}} \mathscr{R}\left(1+(1-\lambda)\nu, \frac{\lambda}{1+(1-\lambda)\nu}, M, c, k\right), \tag{S240}$$

and, in particular, the unconstrained two-way capacities satisfy

$$K(\mathscr{E}_{\lambda,\nu}) \geq Q_2(\mathscr{E}_{\lambda,\nu}) \geq \sup_{c\in(0,1),\, M\in\mathbb{N}^+,\, k\in\mathbb{N}} \mathscr{R}\left(1+(1-\lambda)\nu, \frac{\lambda}{1+(1-\lambda)\nu}, M, c, k\right), \tag{S241}$$

where the quantity $\mathscr{R}$ is defined in (S158).

Proof. Theorem S19 is a direct consequence of Lemma S4 and Theorem S14. □

Theorem S19 shows a new lower bound, reported in (S241), on the two-way capacities of the thermal attenuator $\mathscr{E}_{\lambda,\nu}$. Our new lower bound outperforms all the previous known lower bounds in a large region of the parameters λ and ν. In Fig. 1a and in Fig. 1b we plot our new bound and its ratio with the PLOB bound, respectively, with respect to ν where the transmissivity is chosen to be equal to $\lambda(\nu) := 1 - 2^{-h(\nu)}$, which is the upper endpoint for the λ-range for which the best known lower bound on $Q_2(\mathscr{E}_{\lambda,\nu})$ (i.e. the reverse coherent information lower bound reported in (S34)) vanishes. From Fig. 1a and Fig. 1b we see that for these choices of ν and $\lambda(\nu)$, our new lower bound is now the best lower bound on $Q_2(\mathscr{E}_{\lambda,\nu})$ and it achieves the $\simeq 14\%$ of the PLOB bound for $\nu \gg 1$. For example, if $\nu = 1$ and if the transmissivity is equal to $\lambda = 1 - 2^{-h(1)} = 0.75$, our new lower bound is $\simeq 0.033$, its ratio with the PLOB bound is $\simeq 0.08$, and the optimal parameters of the supremum present in the expression of our new bound in (S241) are $c \simeq 0.703$, $M = 2$, and $k = 2$. In Fig. 2 we plot our new bound on $Q_2(\mathscr{E}_{\lambda,\nu})$ with respect to λ for $\nu = 1$ and $\nu = 10$.

Our new bound can outperform also the best known lower bound (before our work) on the secret-key capacity $K(\mathscr{E}_{\lambda,\nu})$ found by Ottaviani et al. [23]. To demonstrate that our new bound can be strictly tighter than the Ottaviani et al. lower bound, in Fig. 3 we plot the latter bound and our new bound with respect to λ for $\nu = 1$ and $\nu = 10$. From Fig. 3, we note that the Ottaviani et al. lower bound vanishes for larger transmissivities than our bound. In particular, fixed $\nu > 0$, we numerically observe that our new bound is strictly positive for all $\lambda > \frac{\nu}{\nu+1}$, which is the region where the two-way capacities of $\mathscr{E}_{\lambda,\nu}$ are strictly positive, as established by Theorem S12. As an example, for $\nu = 1$, in Fig. 4 we plot the ratio between our bound and the PLOB bound in logarithmic scale and we see that our bound is strictly positive for $\lambda \gtrsim \frac{\nu}{\nu+1} = 0.5$. In addition, fixed $\nu > 0$, we numerically observe that the optimal value of k of the supremum present in the expression of our new bound in (S241) increases as λ decreases and tends to infinity as λ tends to $\frac{\nu}{\nu+1}$, where we recall that k represents the number of iterations of the P1-or-P2 sub-routine [16] in the entanglement distribution protocol we have introduced in the proof of Theorem S13.

We numerically observe that for all λ and ν the optimal choice of M of the supremum present in the expression of our bound in (S241) is always less or equal to 3. Hence, since the mean photon number of each signal sent by Alice is $\mathrm{Tr}[a^\dagger a\, |\Psi_{M,c}\rangle\langle\Psi_{M,c}|] = (1-c^2)M$ (see (S119)), the entanglement distribution protocol we have presented in the proof of Theorem S19 exploits a mean photon number per channel use which is strictly lower than 3. On the contrary, the entanglement distribution protocol which leads to the reverse coherent information lower bound in (S34) requires infinite mean photon number per channel use, as we reviewed in S35.

Theorem S19 shows also the bound in (S240), which constitutes a new lower bound on the EC two-way capacities of the thermal attenuator $\mathscr{E}_{\lambda,\nu}$. This new lower bound can outperform the NPJ lower bound [24] reported in (S38), which is the best known lower bound on the EC two-way capacities of the thermal attenuator, as we show in Fig. 5 where we plot our new bound in (S240) with respect to λ for different choices of ν and of the energy constraint N_s.

By using the results of Section IV, in the forthcoming Theorem S20 we show an additional lower bound on the two-way quantum capacity of the thermal attenuator $\mathscr{E}_{\lambda,\nu}$.

Theorem S20 Multi-rail lower bound**.** *For all $\lambda \in [0,1]$ and $\nu \geq 0$ the two-way capacities of the thermal attenuator $\mathscr{E}_{\lambda,\nu}$ satisfy*

$$K(\mathscr{E}_{\lambda,\nu}) \geq Q_2(\mathscr{E}_{\lambda,\nu}) \geq \sup_{\substack{N,K\in\mathbb{N}^+ \\ K\geq 2}} R\left(1+(1-\lambda)\nu, \frac{\lambda}{1+(1-\lambda)\nu}, N, K\right), \tag{S242}$$

where the quantity R is defined in (S226).

Proof. Theorem S20 is a direct consequence of Theorem S17 and Lemma S4. □

Theorem S20 shows an additional lower bound on $Q_2(\mathscr{E}_{\lambda,\nu})$, that we dub 'multi-rail lower bound'. This bound is the ebit rate of the entanglement distribution protocol presented in Section IV, which combines the multi-rail protocol introduced in [61] and the qudit P1-or-P2 protocol introduced in [16]. In Fig. 6 we plot both the multi-rail lower bound (reported in (S242)) and our previously discussed lower bound (reported in (S241)) as a function of λ for $\nu = 0.1$, $\nu = 0.5$, $\nu = 1$, and $\nu = 10$. Our numerical investigation shows that for $\nu \lesssim 1$, the multi-rail lower bound is tighter than the previously discussed lower bound, as confirmed by Fig. 6.

B. Results on the two-way capacities of the thermal amplifier

Let us consider the thermal amplifier $\Phi_{g,\nu}$ of gain $g \geq 1$ and thermal noise $\nu \geq 0$. Since the PLOB bound in (S49) vanishes for $g \geq 1 + \frac{1}{\nu}$, it is already known that the two-way capacities of $\Phi_{g,\nu}$ vanish for $g \geq 1 + \frac{1}{\nu}$. The following theorem establishes that also the vice-versa is true.

Theorem S21. *Let $g \geq 1$, $\nu \geq 0$, and $N_s > 0$. The energy-constrained two-way capacities of the thermal amplifier $Q_2(\Phi_{g,\nu}, N_s)$ and $K(\Phi_{g,\nu}, N_s)$ vanish if and only if $g \geq 1 + \frac{1}{\nu}$, i.e. if and only if $\Phi_{g,\nu}$ is entanglement breaking. In particular, the same holds for the unconstrained two-way capacities.*

Proof. Theorem S21 is a direct consequence of Lemma S4 and Theorem S12. □

Except for the special case $\nu = 0$, it is an open question whether the coherent information lower bound in Eq. S50 equals the true two-way quantum capacity of the thermal amplifier $Q_2(\Phi_{g,\nu})$: Theorem S21 provides a negative answer to this question. Indeed, although $Q_2(\Phi_{g,\nu}) = 0$ if and only if $g > 1 + \frac{1}{\nu}$ (thanks to Theorem S21), the coherent information lower bound vanishes for all $g \geq \frac{1}{1-2^{-h(\nu)}}$. Hence, since $1 + \frac{1}{\nu} > \frac{1}{1-2^{-h(\nu)}}$ for all $\nu > 0$, the coherent information lower bound is not equal to $Q_2(\Phi_{g,\nu})$ at least in the region $\nu > 0$ and $g \in [\frac{1}{1-2^{-h(\nu)}}, 1 + \frac{1}{\nu})$. In the following theorem we obtain an improved lower bound on the two-way capacities of the thermal amplifier.

Theorem S22. *Let $g \geq 1$, $\nu \geq 0$, and $N_s \geq 0$. The EC two-way capacities $Q_2(\Phi_{g,\nu}, N_s)$ and $K(\Phi_{g,\nu}, N_s)$ of the thermal amplifier $\Phi_{g,\nu}$ satisfy the following lower bound*

$$K(\Phi_{g,\nu}, N_s) \geq Q_2(\Phi_{g,\nu}, N_s) \geq \sup_{\substack{c\in(0,1),\, M\in\mathbb{N}^+,\, k\in\mathbb{N} \\ (1-c^2)M \leq N_s}} \mathscr{R}\left(g + (g-1)\nu, \frac{g}{g+(g-1)\nu}, M, c, k\right), \tag{S243}$$

and, in particular, the unconstrained two-way capacities satisfy

$$K(\Phi_{g,\nu}) \geq Q_2(\Phi_{g,\nu}) \geq \sup_{c\in(0,1),\, M\in\mathbb{N}^+,\, k\in\mathbb{N}} \mathscr{R}\left(g + (g-1)\nu, \frac{g}{g+(g-1)\nu}, M, c, k\right), \tag{S244}$$

where the quantity $\mathscr{R}$ is defined in (S158).

Proof. Theorem S22 is a direct consequence of Lemma S4 and Theorem S14. □

Theorem S22 shows a new lower bound, reported in (S244), on the two-way capacities of the thermal amplifier $\Phi_{g,\nu}$. Our new lower bound outperforms all the previous known lower bounds in a large region of the parameters g and ν. In Fig. 7a and in Fig. 7b we plot our new bound and its ratio with the PLOB bound, respectively, with respect to ν where the transmissivity is chosen to be equal to $g(\nu) := \frac{1}{1-2^{-h(\nu)}}$, which is the lower endpoint for the g-range for which the best known lower bound on $Q_2(\Phi_{g,\nu})$ (i.e. the coherent information lower bound reported in (S50)) vanishes. From Fig. 7a and Fig. 7b we see that for these choices of ν and $g(\nu)$, our new lower bound is now the best lower bound on $Q_2(\Phi_{g,\nu})$ and it achieves the $\simeq 14\%$ of the PLOB bound for $\nu \gg 1$. In Fig. 8 we plot our new bound with respect to g for $\nu = 1$ and $\nu = 10$.

Our new bound can outperform also the WOGP-bound [27], which is the best known lower bound (before our work) on the secret-key capacity $K(\Phi_{g,\nu})$. To demonstrate that our new bound can be strictly tighter than the WOGP lower bound, in Fig. 9 we plot the latter bound and our new bound with respect to g for $\nu = 1$ and $\nu = 10$. From Fig. 9 we note that the WOGP lower bound vanishes for smaller values of g than our bound. In particular, fixed $\nu > 0$, we numerically observe that our new bound is strictly positive for all $g < 1 + \frac{1}{\nu}$, which is the region where the two-way capacities of $\Phi_{g,\nu}$ are strictly positive, as established by Theorem S21. As an example, for $\nu = 1$, in Fig. 10 we plot the ratio between our bound and the PLOB bound in logarithmic scale and we see that our bound is strictly positive for $g \lesssim 1 + \frac{1}{\nu} = 2$.

C. Results on the two-way capacities of the additive Gaussian noise

Let us consider the additive Gaussian noise Λ_ξ of parameter $\xi \geq 0$. Since the PLOB bound in (S61) vanishes for $\xi \geq 1$, it is already known that the two-way capacities of Λ_ξ vanish for $\xi \geq 1$. The following theorem establishes that also the vice-versa is true.

Theorem S23. *Let $\xi \geq 0$, and $N_s > 0$. The energy-constrained two-way capacities of the additive Gaussian noise $Q_2(\Lambda_\xi, N_s)$ and $K(\Lambda_\xi, N_s)$ vanish if and only if $\xi \geq 1$. In particular, the two-way capacities $Q_2(\Lambda_\xi)$ and $K(\Lambda_\xi)$ vanish if and only if $\xi \geq 1$.*

Proof. Theorem S23 is a direct consequence of Lemma S4 and Theorem S12. □

It is an open question whether the coherent information lower bound in Eq. S62 equals the true two-way quantum capacity of the additive Gaussian noise $Q_2(\Lambda_\xi)$: Theorem S23 provides a negative answer to this question. Indeed, although $Q_2(\Lambda_\xi) = 0$ if and only if $\xi \geq 1$ (thanks to Theorem S23), the coherent information lower bound vanishes for all $\xi \geq \frac{1}{e}$. Hence, the coherent information lower bound is not equal to $Q_2(\Lambda_\xi)$ at least in the region $\xi \in [\frac{1}{e}, 1)$. In the following theorem we obtain an improved lower bound on the two-way capacities of the additive Gaussian noise.

Theorem S24. *Let $\xi \in [0, 1)$ and $N_s \geq 0$. The EC two-way capacities $Q_2(\Lambda_\xi, N_s)$ and $K(\Lambda_\xi, N_s)$ of the additive Gaussian noise Λ_ξ satisfy the following lower bound*

$$K(\Lambda_\xi, N_s) \geq Q_2(\Lambda_\xi, N_s) \geq \sup_{\substack{c\in(0,1),\, M\in\mathbb{N}^+,\, k\in\mathbb{N} \\ (1-c^2)M \leq N_s}} \mathscr{R}\left(1+\xi, \frac{1}{1+\xi}, M, c, k\right), \tag{S245}$$

and, in particular, the unconstrained two-way capacities satisfy

$$K(\Lambda_\xi) \geq Q_2(\Lambda_\xi) \geq \sup_{c\in(0,1),\, M\in\mathbb{N}^+,\, k\in\mathbb{N}} \mathscr{R}\left(1+\xi, \frac{1}{1+\xi}, M, c, k\right), \tag{S246}$$

where the quantity $\mathscr{R}$ is defined in (S158).

Proof. Theorem S24 is a direct consequence of Lemma S4 and Theorem S14. □

Theorem S24 shows a new lower bound, reported in (S246), on the two-way capacities of the additive Gaussian noise Λ_ξ. Our new lower bound outperforms all the previous known lower bounds in a large region of the parameter ξ, as it can been seen from Fig. 11.

---

[1] A. Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods.* CRC Press, Taylor & Francis Group, Boca Raton, USA, 2017.

[2] R. Simon. Peres–Horodecki separability criterion for continuous variable systems. *Phys. Rev. Lett.*, 84:2726–2729, 2000.

[3] M. M. Wilde. *Quantum Information Theory.* Cambridge University Press, 2nd edition, 2017.

[4] A. S. Holevo. Entanglement-breaking channels in infinite dimensions. *Probl. Pered. Inform.*, 44(3):3–18, 2008. (English translation: Probl. Inf. Transm. 44(3):171–184, 2008).

[5] S. Khatri and M. M. Wilde. Principles of quantum communication theory: A modern approach, 2020.

[6] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[7] H. Dür and Briegel H. J. Entanglement purification and quantum error correction. *Reports on Progress in Physics*, 70(8):1381–1424, 2007.

[8] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proc. Royal Soc. A*, 461(2053):207–235, 2005.

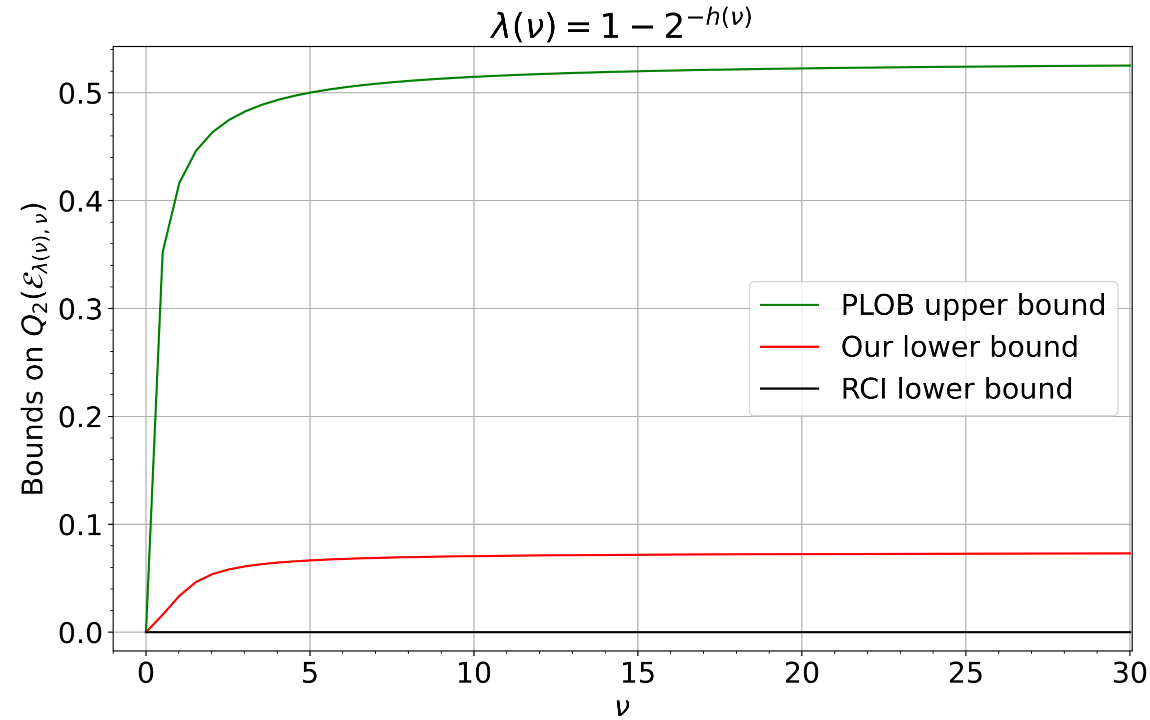
[9] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, 1996.

[10] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722–725, 1996.

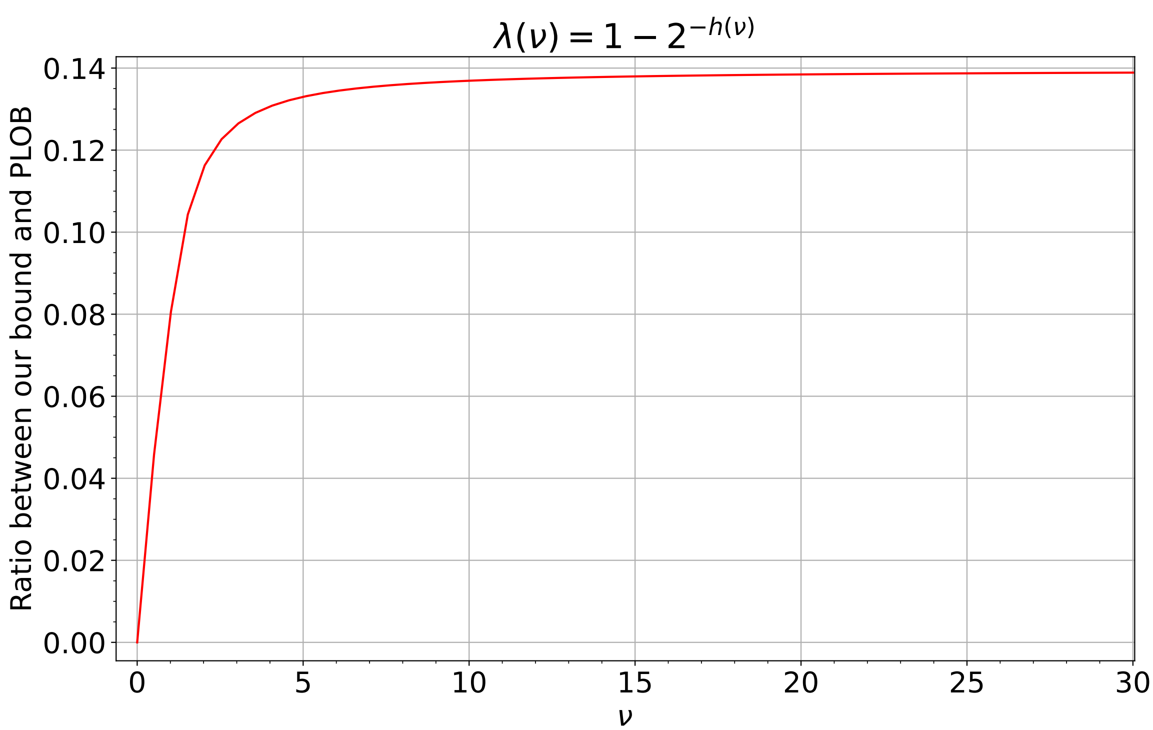
[11] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77:2818–2821, 1996.

[12] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete. Local permutations of products of bell states and entanglement distillation. *Phys. Rev. A*, 67:022310, 2003.

[13] M. Horodecki and P. Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Phys. Rev. A*, 59:4206–4216, 1999.



(a)

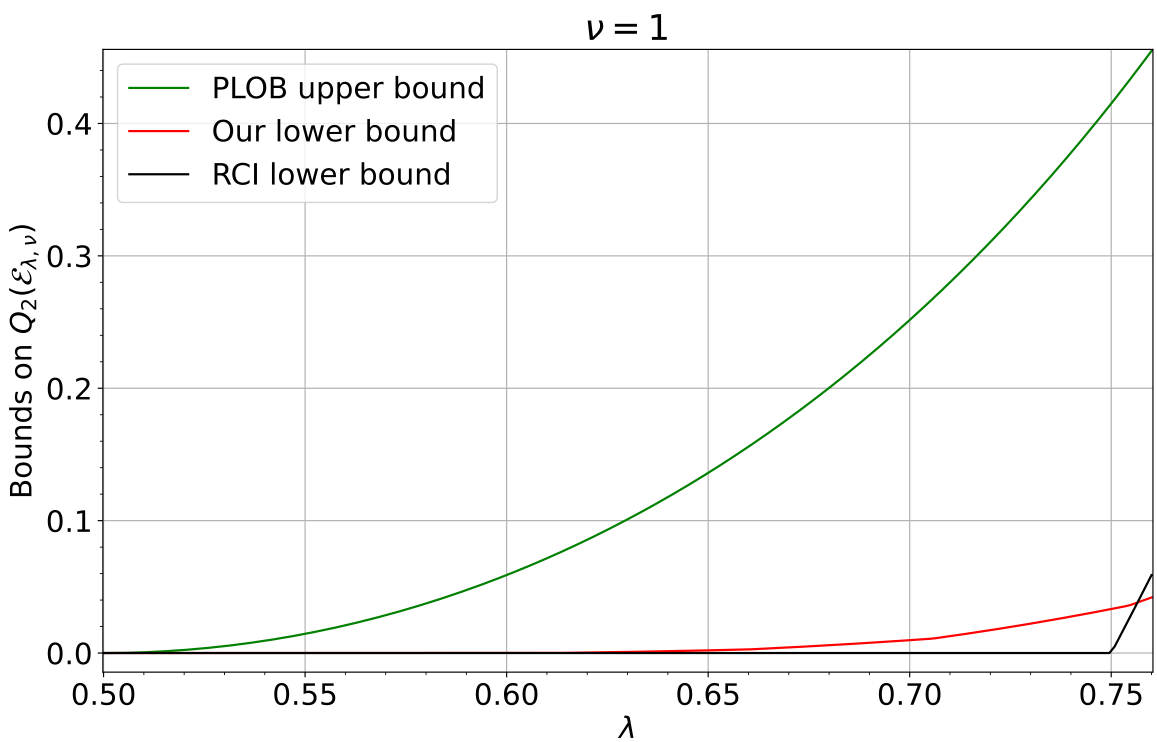


(b)

FIG. 1. **(a).** Bounds on the two-way quantum capacity of the thermal attenuator $Q_2(\mathscr{E}_{\lambda(\nu),\nu})$ plotted with respect to ν, where the transmissivity is equal to the critical value $\lambda(\nu) \coloneqq 1 - 2^{-h(\nu)}$. The red curve is our lower bound calculated by exploiting (S241). The black curve is the best known lower bound on $Q_2(\mathscr{E}_{\lambda(\nu),\nu})$, which is the reverse coherent information lower bound reported in (S34) (which is zero since $\lambda(\nu) = 1 - 2^{-h(\nu)}$). The green curve is the PLOB upper bound reported in (S32). These bounds are also bounds on the secret-key capacity $K(\mathscr{E}_{\lambda(\nu),\nu})$. **(b).** Ratio between our new lower bound on the two-way quantum and secret-key capacities in (S241) and the PLOB bound in (S32) as a function of ν where the transmissivity is $\lambda(\nu) \coloneqq 1 - 2^{-h(\nu)}$.

[14] G. Alber, A. Delgado, N. Gisin, and I. Jex. Efficient bipartite quantum state purification in arbitrary dimensional hilbert spaces. *Journal of Physics A: Mathematical and General*, 34(42):8821–8833, 2001.
[15] H. Bombin and M. A. Martin-Delgado. Entanglement distillation protocols and number theory. *Phys. Rev. A*, 72:032313, 2005.
[16] J. Miguel-Ramiro and W. Dür. Efficient entanglement purification protocols for d-level systems. *Phys. Rev. A*, 98:042309, 2018.
[17] K. G. H. Vollbrecht and F. Verstraete. Interpolation of recurrence and hashing entanglement distillation protocols. *Phys. Rev. A*, 71:062325, 2005.
[18] E. Hostens, J. Dehaene, and B. De Moor. Asymptotic adaptive bipartite entanglement-distillation protocol. *Phys. Rev. A*, 73:062337, 2006.
[19] S. Barnett and P. M. Radmore. *Methods in Theoretical Quantum Optics.* Oxford Series in Optical and Imaging Sciences. Clarendon Press, 2002.
[20] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nat. Commun.*, 8(1):15043, 2017.
[21] A. S. Holevo and V. Giovannetti. Quantum channels and their entropic characteristics. *Reports on Progress in Physics*, 75(4):046001, 2012.
[22] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.*, 102:050503, 2009.
[23] C. Ottaviani, R. Laurenza, T. P. W. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola. Secret key capacity of the thermal-loss channel: improving the lower bound. In M. T. Gruneisen, M. Dusek, and J. G. Rarity, editors, *Quantum Information Science and Technology II*, volume 9996, page 999609. International Society for Optics and Photonics, SPIE, 2016.
[24] K. Noh, S. Pirandola, and L. Jiang. Enhanced energy-constrained quantum communication over bosonic Gaussian channels. *Nat. Commun.*, 11(1):457, 2020.
[25] N. Davis, M. E. Shirokov, and M. M. Wilde. Energy-constrained two-way assisted private and quantum capacities of quantum channels. *Phys. Rev. A*, 97:062310, 2018.
[26] A. S. Holevo and R. F. Werner. Evaluating capacities of bosonic Gaussian channels. *Phys. Rev. A*, 63:032312, 2001.
[27] G. Wang, C. Ottaviani, H. Guo, and S. Pirandola. Improving the lower bound to the secret-key capacity of the thermal amplifier channel. *The European Physical Journal D*, 73(1):17, 2019.
[28] C. D. Cushen and R. L. Hudson. A quantum-mechanical central limit theorem. *Journal of Applied Probability*, 8(3):454–469, 1971.
[29] F. A. Mele, L. Lami, and V. Giovannetti. Quantum optical communication in the presence of strong attenuation noise. *Phys. Rev. A*, 106:042437, 2022.
[30] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi. Theory of channel simulation and bounds for private communication. *Quantum Science and Technology*, 3(3):035009, 2018.
[31] A. S. Holevo. The Choi–Jamiolkowski forms of quantum Gaussian channels. *J. Math. Phys.*, 52(4):042202, 2011.
[32] A. S. Holevo. On the Choi–Jamiolkowski correspondence in infinite dimensions. *Preprint arXiv:1004.0196*, 2010.
[33] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, 1996.
[34] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac. Entanglement criteria for all bipartite Gaussian states. *Phys. Rev. Lett.*, 87:167904, 2001.
[35] K. Goodenough, D. Elkouss, and S. Wehner. Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels. *New Journal of Physics*, 18(6):063005, 2016.
[36] M. Horodecki, P. Horodecki, and R. Horodecki. Inseparable two spin-$\frac{1}{2}$ density matrices can be distilled to a singlet form. *Phys. Rev. Lett.*, 78:574–577, 1997.
[37] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.*, 125:010502, 2020.
[38] A. A. E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring. Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator. *Science Advances*, 10(1):eadi9474, 2024.
[39] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo. Continuous-variable QKD over 50 km commercial fiber. *Quantum Science and Technology*, 4(3):035006, 2019.
[40] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and B. Xu. Sub-mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber. *Optics Letters*, 48(7):1766, 2023.
[41] D. Huang, P. Huang, D. Lin, and G. Zeng. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports*, 6:19201, 01 2016.
[42] E. Bersin, M. Sutula, Y. Q. Huan, A. Suleymanzade, D. R. Assumpcao, Y.-C. Wei, P.-J. Stas, C. M. Knaut, E. N. Knall, C. Langrock, N. Sinclair, R. Murphy, R. Riedinger, M. Yeh, C. J. Xin, S. Bandyopadhyay, D. D. Sukachev, B. Machielse, D. S. Levonian, M. K. Bhaskar, S. Hamilton, H. Park, M. Lončar, M. M. Fejer, P. B. Dixon, D. R. Englund, and M. D. Lukin. Telecom networking with a diamond quantum memory. *PRX Quantum*, 5:010303, 2024.
[43] A. Wallucks, I. Marinkovic, B. Hensen, R. Stockill, and S. Groblacher. A quantum memory at telecom wavelengths. *Nat. Phys.*, 16(7):772–777, 2020.
[44] N. N. Kalb, A. A. A. A. Reiserer, P. C. Humphreys, J. J. W. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson. Entanglement distillation between solid-state quantum network nodes. *Science*, 356(6341):928–932, 2017.

[45] X.-M. Hu, C.-X. Huang, Y.-B. Sheng, L. Zhou, B.-H. Liu, Y. Guo, C. Zhang, W.-B. Xing, Y.-F. Huang, C.-F. Li, and G.-C. Guo. Long-distance entanglement purification for quantum communication. *Phys. Rev. Lett.*, 126(1), 2021.
[46] S. Ecker, P. Sohr, L. Bulla, M. Huber, M. Bohmann, and R. Ursin. Experimental single-copy entanglement distillation. *Phys. Rev. Lett.*, 127(4), 2021.
[47] B. C. Sanders. Quantum dynamics of the nonlinear rotator and the effects of continual spin measurement. *Phys. Rev. A*, 40:2417–2427, 1989.
[48] G. J. Pryde and A. G. White. Creation of maximally entangled photon-number states using optical fiber multiports. *Phys. Rev. A*, 68(5), 2003.
[49] I. Afek, O. Ambar, and Y. Silberberg. High-NOON states by mixing quantum and classical light. *Science*, 328(5980):879–881, 2010.
[50] L. Liang, G. W. Lin, Y. M. Hao, Y. P. Niu, and S. Q. Gong. Quantum nondemolition measurement of small photon numbers using stored light. *Phys. Rev. A*, 90:055801, Nov 2014.
[51] A. Cabello and F. Sciarrino. Loophole-free Bell test based on local precertification of photon's presence. *Phys. Rev. X*, 2:021010, 2012.
[52] A. V. Gorshkov, R. Nath, and T. Pohl. Dissipative many-body quantum optics in Rydberg media. *Phys. Rev. Lett.*, 110:153601, 2013.
[53] G.-S. Ye, B. Xu, Y. Chang, S. Shi, T. Shi, and L. Li. A photonic entanglement filter with Rydberg atoms. *Nat. Photonics*, 17(6):538–543, 2023.
[54] J. Honer, R. Löw, H. Weimer, T. Pfau, and H. P. Büchler. Artificial atoms can do more than atoms: Deterministic single photon subtraction from arbitrary light fields. *Phys. Rev. Lett.*, 107:093601, 2011.
[55] N. Stiesdal, H. Busche, K. Kleinbeck, J. Kumlin, M. G. Hansen, H. P. Büchler, and S. Hofferberth. Controlled multi-photon subtraction with cascaded Rydberg superatoms as single-photon absorbers. *Nat. Commun.*, 12(1), 2021.
[56] M. Mücke, E. Figueroa, J. Bochmann, C. Hahn, K. Murr, S. Ritter, C. Villas-Boas, and G. Rempe. Electromagnetically induced transparency with single atoms in a cavity. *Nature*, 465:755–8, 06 2010.
[57] S. Rosenblum, O. Bechler, I. Shomroni, Y. Lovsky, G. Guendelman, and B. Dayan. Extraction of a single photon from an optical pulse. *Nat. Photonics*, 10(1):19–22, 2015.
[58] A. Kumar, A. Suleymanzade, M. Stone, L. Taneja, A. Anferov, D. I. Schuster, and J. Simon. Quantum-enabled millimetre wave to optical transduction using neutral atoms. *Nature*, 615(7953):614–619, 2023.
[59] J. Rochman, T. Xie, J. G. Bartholomew, K. C. Schwab, and A. Faraon. Microwave-to-optical transduction with erbium ions coupled to planar photonic and superconducting resonators. *Nature Commun.*, 14(1):1153, 2023.
[60] Y. Xu, A. Al Sayem, L. Fan, C.-L. Zou, S. Wang, R. Cheng, W. Fu, L. Yang, M. Xu, and H. X. Tang. Bidirectional interconversion of microwave and light with thin-film lithium niobate. *Nat. Commun.*, 12, 2021.
[61] M. S. Winnel, J. J. Guanzon, N. Hosseinidehaj, and T. C. Ralph. Achieving the ultimate end-to-end rates of lossy quantum communication networks. *arXiv:2203.13924*, 2022.
[62] S. Pirandola et al. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236, 2020.



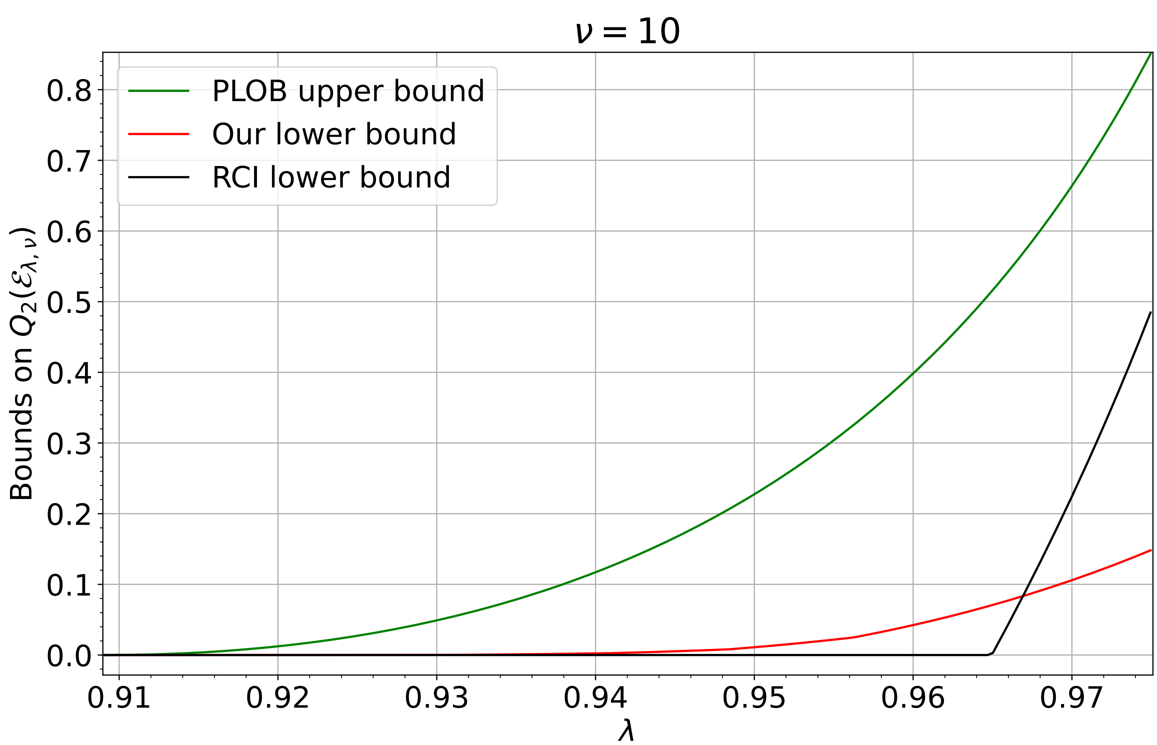


FIG. 2. Bounds on the two-way quantum capacity of the thermal attenuator $Q_2(\mathscr{E}_{\lambda,\nu})$ plotted with respect to λ. The red line is our new lower bound obtained by exploiting (S241). The black line is the best known lower bound on $Q_2(\mathscr{E}_{\lambda,\nu})$, which is the reverse coherent information lower bound reported in (S34). The green line is the PLOB upper bound reported in (S32). These bounds are also bounds on the secret-key capacity $K(\mathscr{E}_{\lambda,\nu})$.

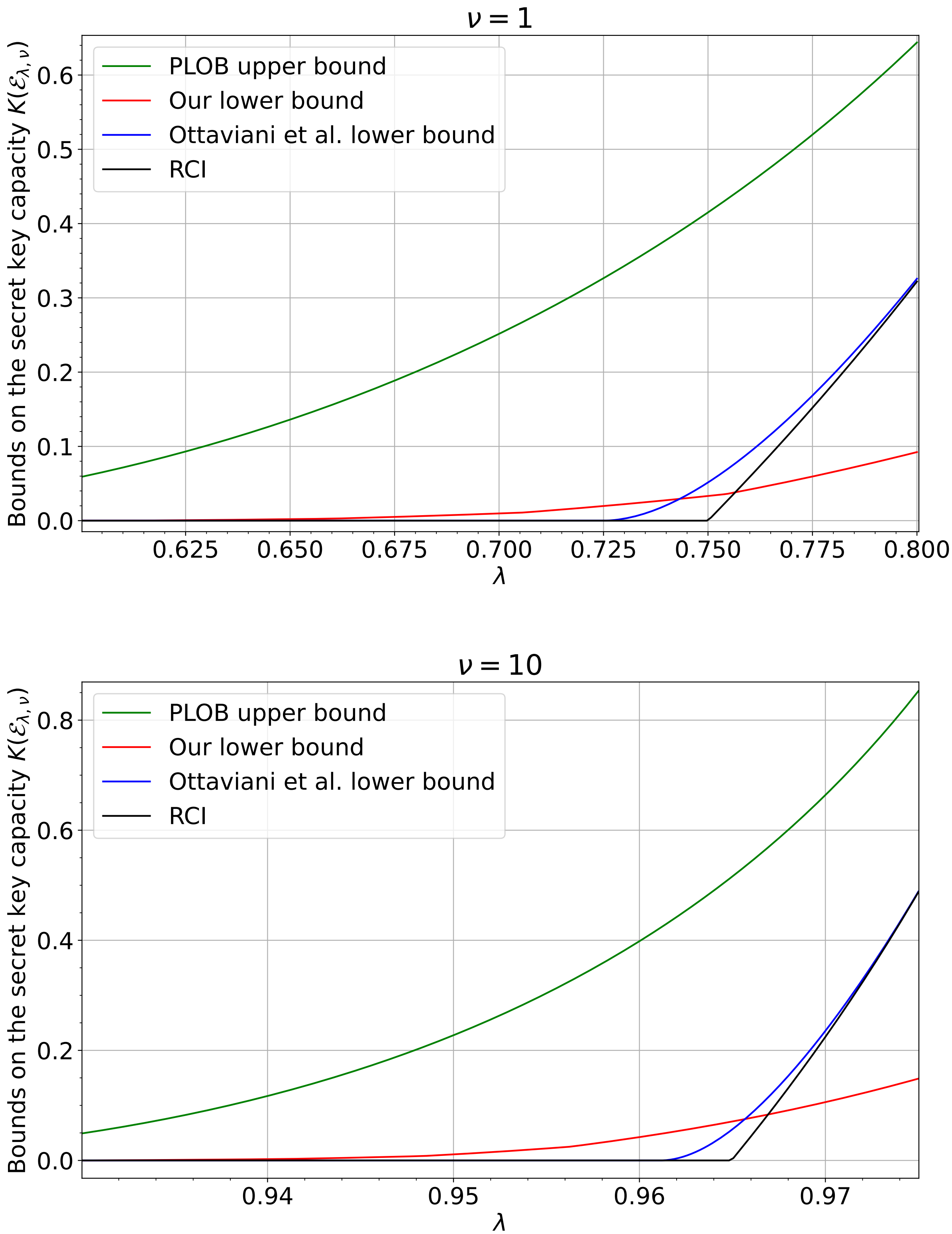


FIG. 3. Bounds on the secret-key capacity of the thermal attenuator $K(\mathscr{E}_{\lambda,\nu})$ plotted with respect to λ. The red line is our new lower bound obtained by exploiting (S241), the black line is the bound in (S34) calculated by evaluating the reverse coherent information in (S35), the blue line is the best known lower bound discovered by [23], and the green line is the PLOB upper bound reported in (S32).

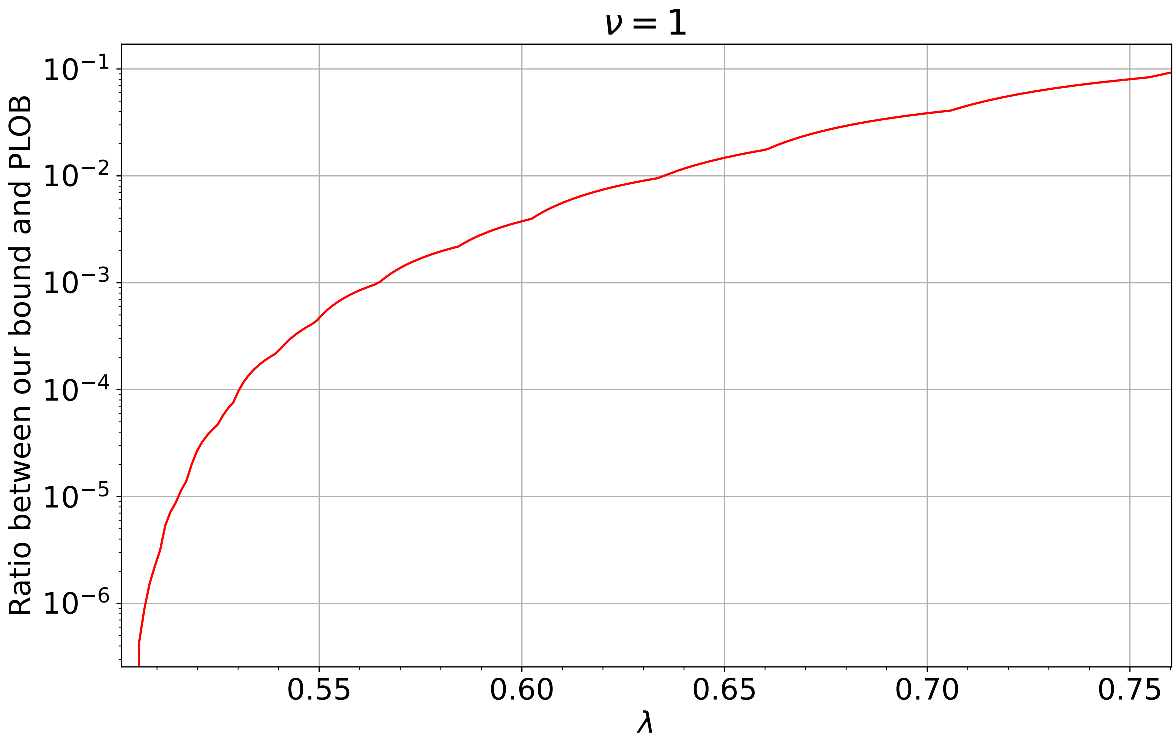


FIG. 4. Ratio between our lower bound on the two-way quantum and secret-key capacities of the thermal attenuator in (S241) and the PLOB bound in (S32) as a function of λ for $\nu = 1$.

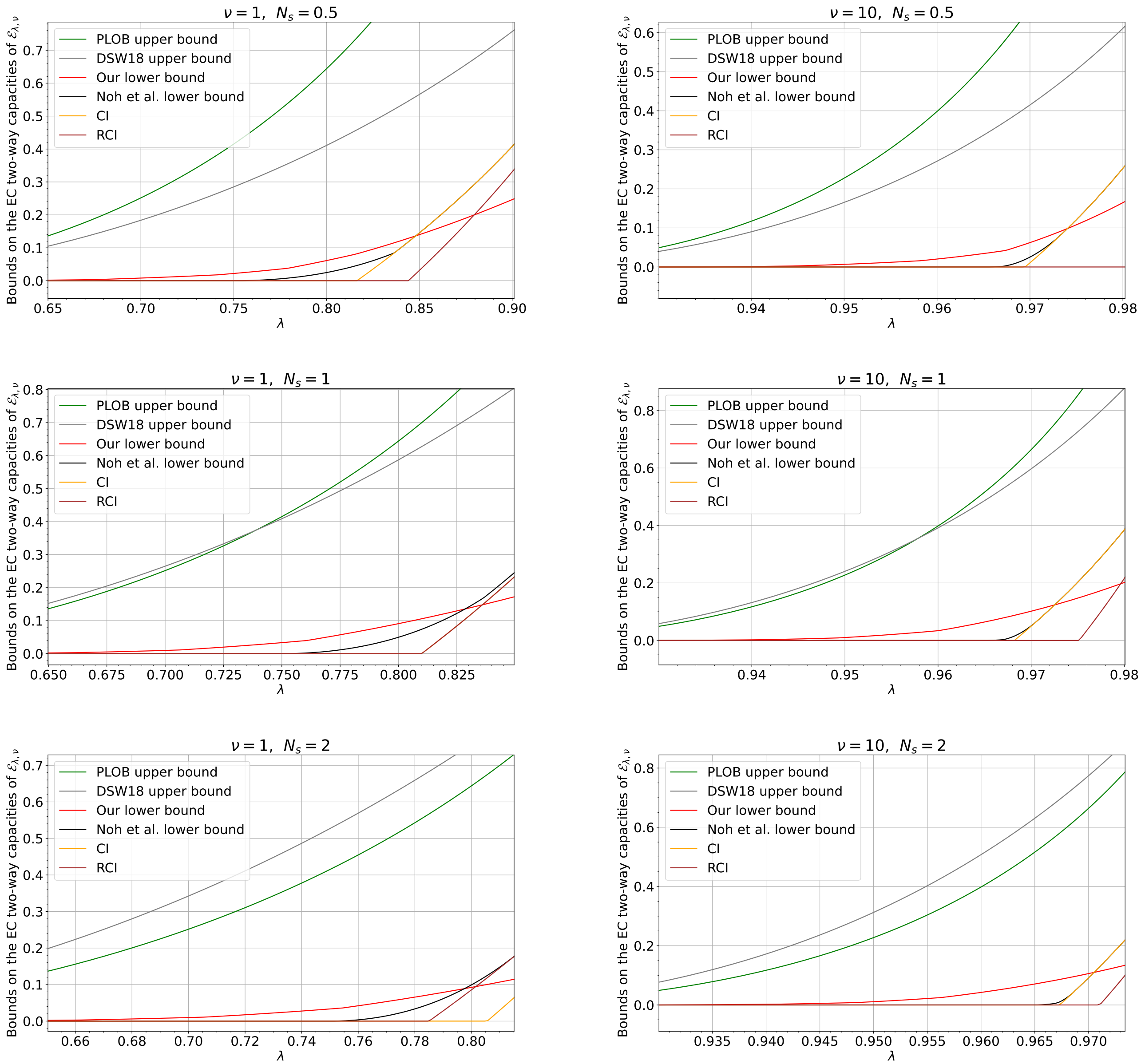


FIG. 5. Bounds on the energy-constrained two-way quantum capacity $Q_2(\mathscr{E}_{\lambda,\nu}, N_s)$ and secret-key capacity $K(\mathscr{E}_{\lambda,\nu}, N_s)$ of the thermal attenuator plotted with respect to λ for different choices of ν and of the energy constraint N_s. The red line is our new lower bound obtained by exploiting (S240), the black line is the NPJ lower bound [24] reported in (S38), the yellow line is the coherent information lower bound reported in (S37), the brown line is the reverse coherent information lower bound reported in (S37), the grey line is the DSW18 upper bound [25], and the green line is the PLOB upper bound reported in (S32).

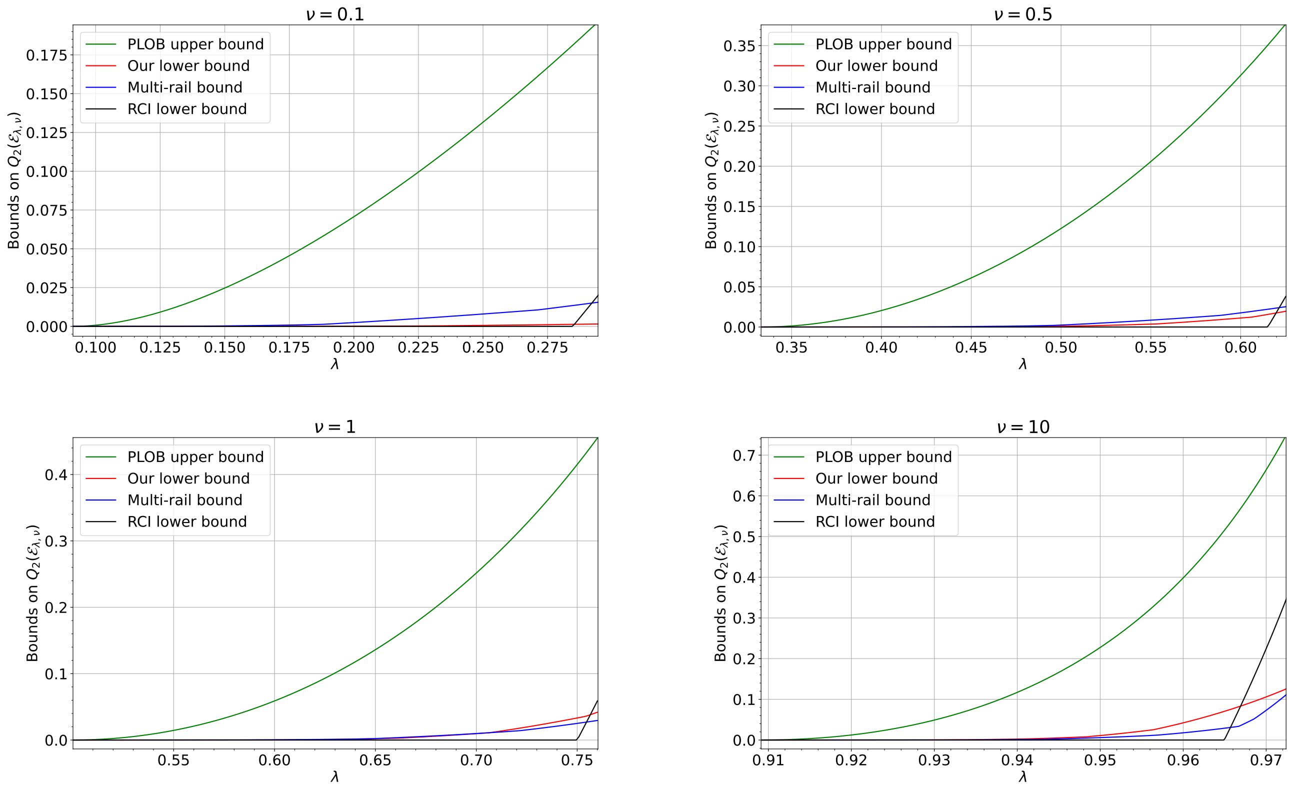
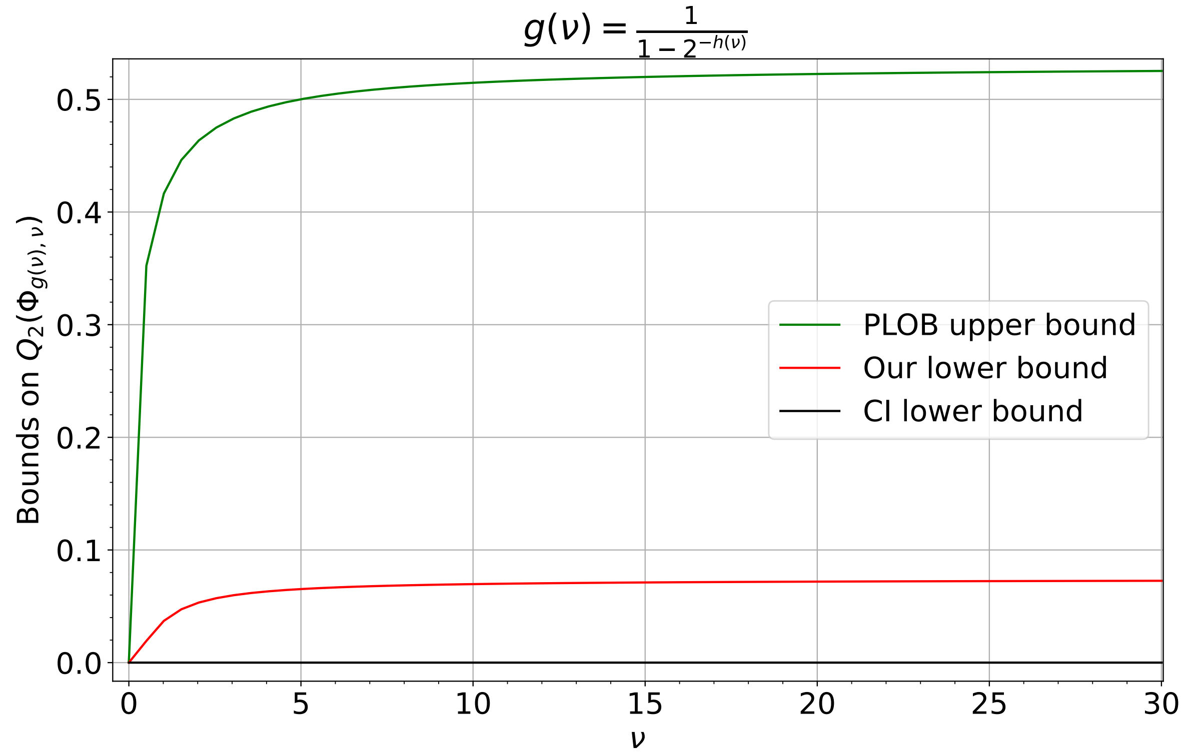
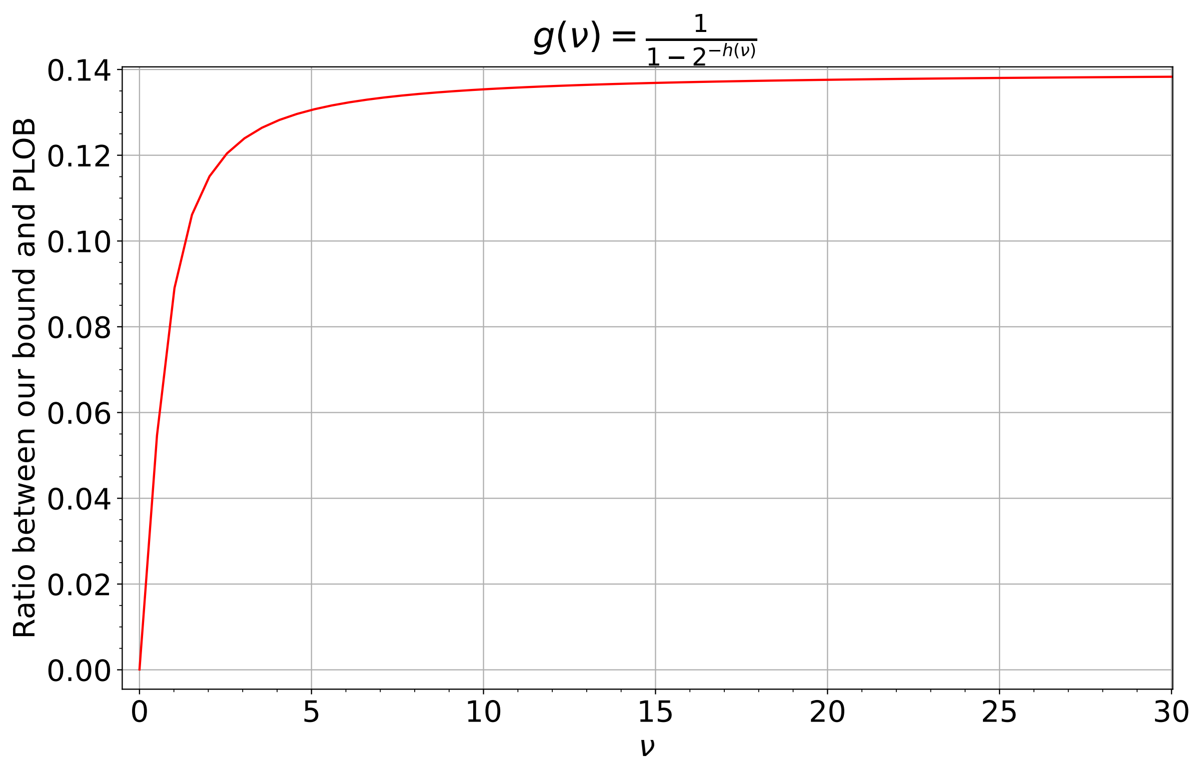


FIG. 6. Bounds on the two-way quantum capacity of the thermal attenuator $Q_2(\mathscr{E}_{\lambda,\nu})$ plotted with respect to λ. The blue line is our multi-rail lower bound obtained by exploiting (S242). The red line is our lower bound reported in (S241). The black line is the best known lower bound on $Q_2(\mathscr{E}_{\lambda,\nu})$, which is the reverse coherent information lower bound reported in (S34). The green line is the PLOB upper bound reported in (S32). These bounds are also bounds on the secret-key capacity $K(\mathscr{E}_{\lambda,\nu})$.



(a)



(b)

FIG. 7. **(a).** Bounds on the two-way quantum capacity of the thermal amplifier $Q_2(\Phi_{g(\nu),\nu})$ plotted with respect to ν, where the gain is equal to the critical value $g(\nu) = \frac{1}{1-2^{-h(\nu)}}$. The red curve is our new lower bound calculated by exploiting (S244). The black curve is the best known lower bound, i.e. the coherent information lower bound reported in (S50) (which is zero since $g(\nu) = \frac{1}{1-2^{-h(\nu)}}$). The green curve is the PLOB upper bound reported in (S49). These bounds are also bounds on the secret-key capacity $K(\Phi_{g(\nu),\nu})$. **(b).** Ratio between our new lower bound in (S244) and the PLOB bound in (S49) as a function of ν where the gain is $g(\nu) := \frac{1}{1-2^{-h(\nu)}}$.

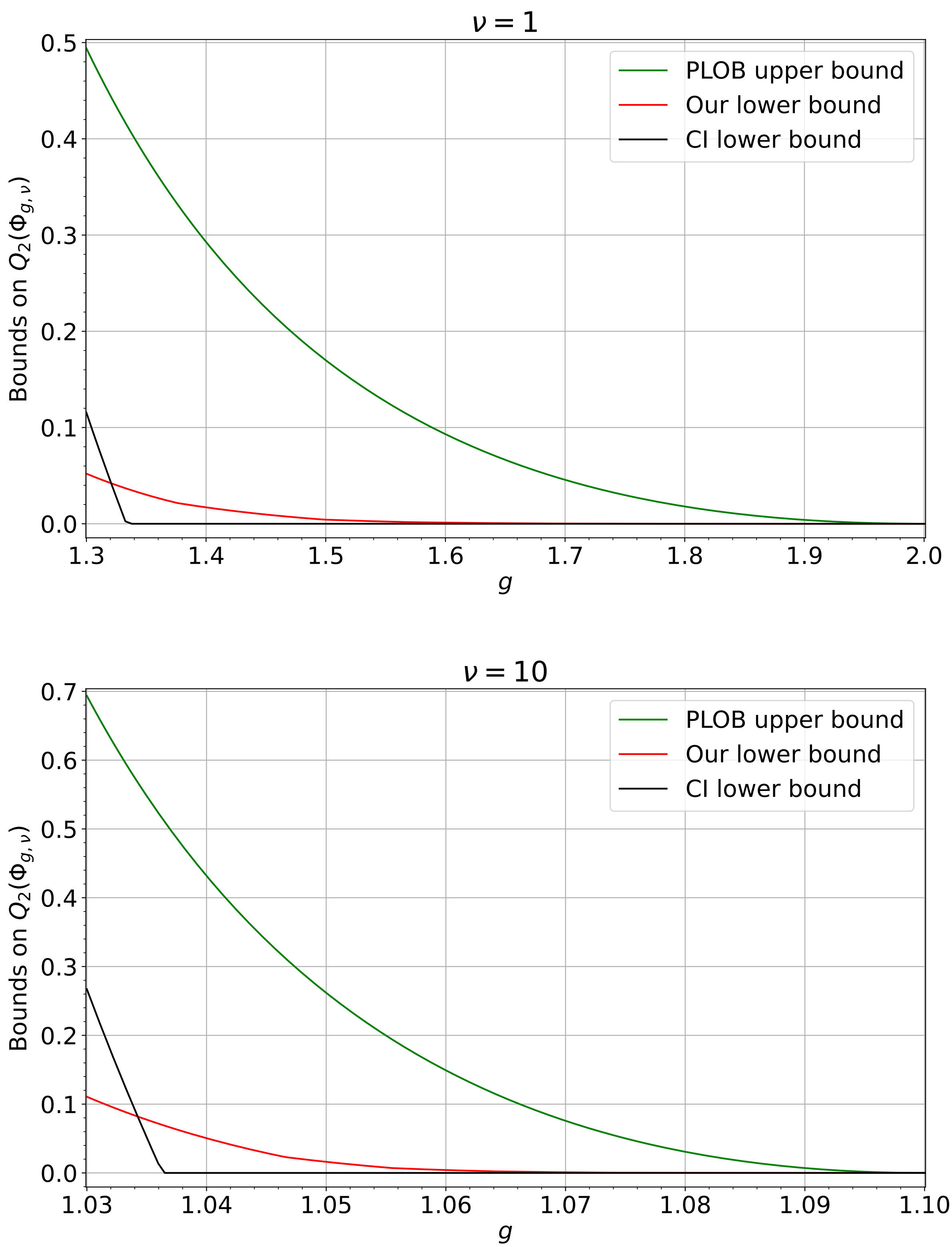


FIG. 8. Bounds on the two-way quantum capacity of thermal amplifier $Q_2(\Phi_{g,\nu})$ plotted with respect to g. The red line is our new lower bound obtained by exploiting (S244). The black line is the best known lower bound on $Q_2(\Phi_{g,\nu})$, which is the coherent information lower bound reported in (S50). The green line is the PLOB upper bound reported in (S49). These bounds are also bounds on the secret-key capacity $K(\Phi_{g,\nu})$.

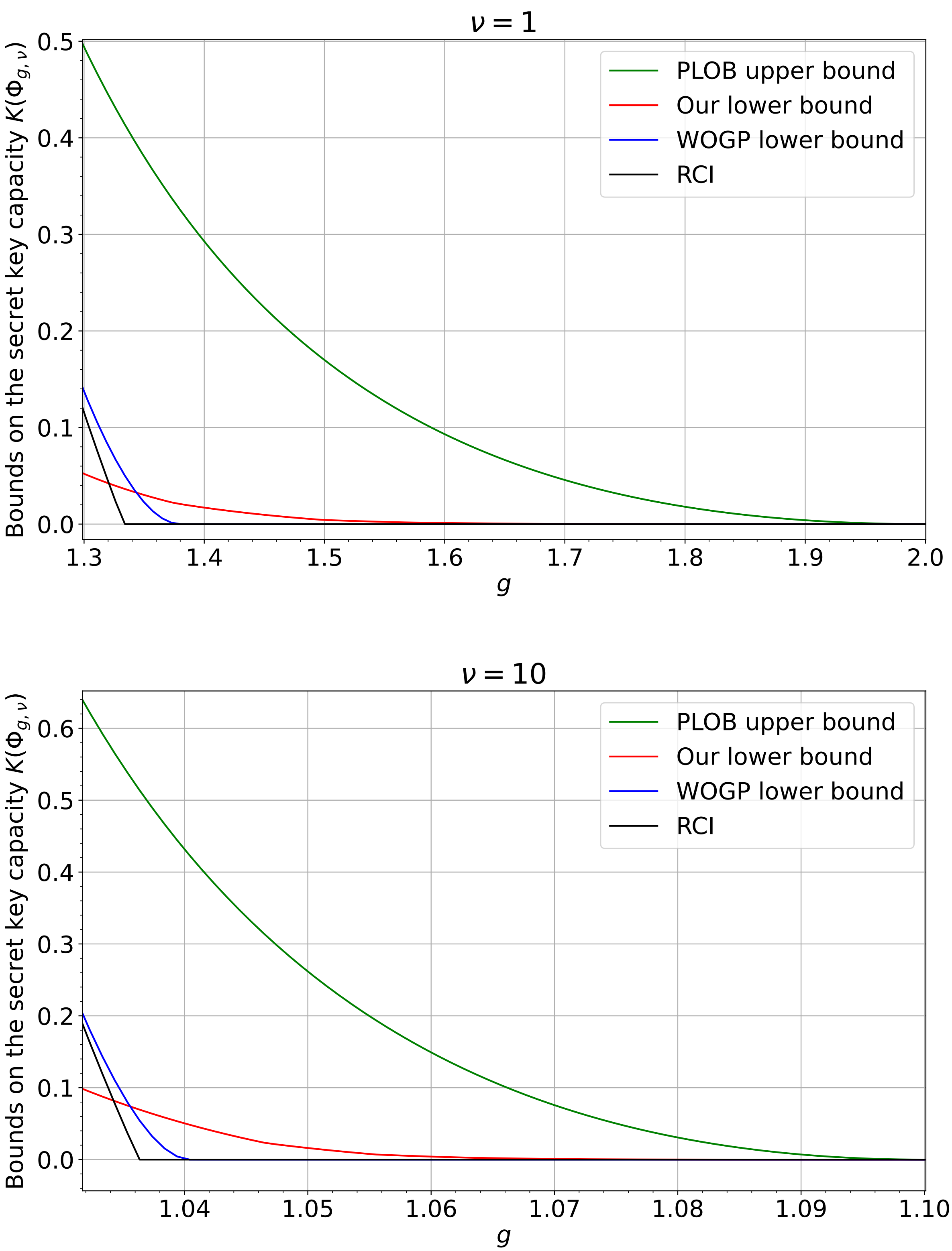


FIG. 9. Bounds on the secret-key capacity of the thermal amplifier $K(\Phi_{g,\nu})$ plotted with respect to g. The red line is our new lower bound obtained by exploiting (S244), the black line is the bound in (S50) calculated by evaluating the coherent information in (S51), the blue line is the WOGP lower bound [23], and the green line is the PLOB upper bound reported in (S49).

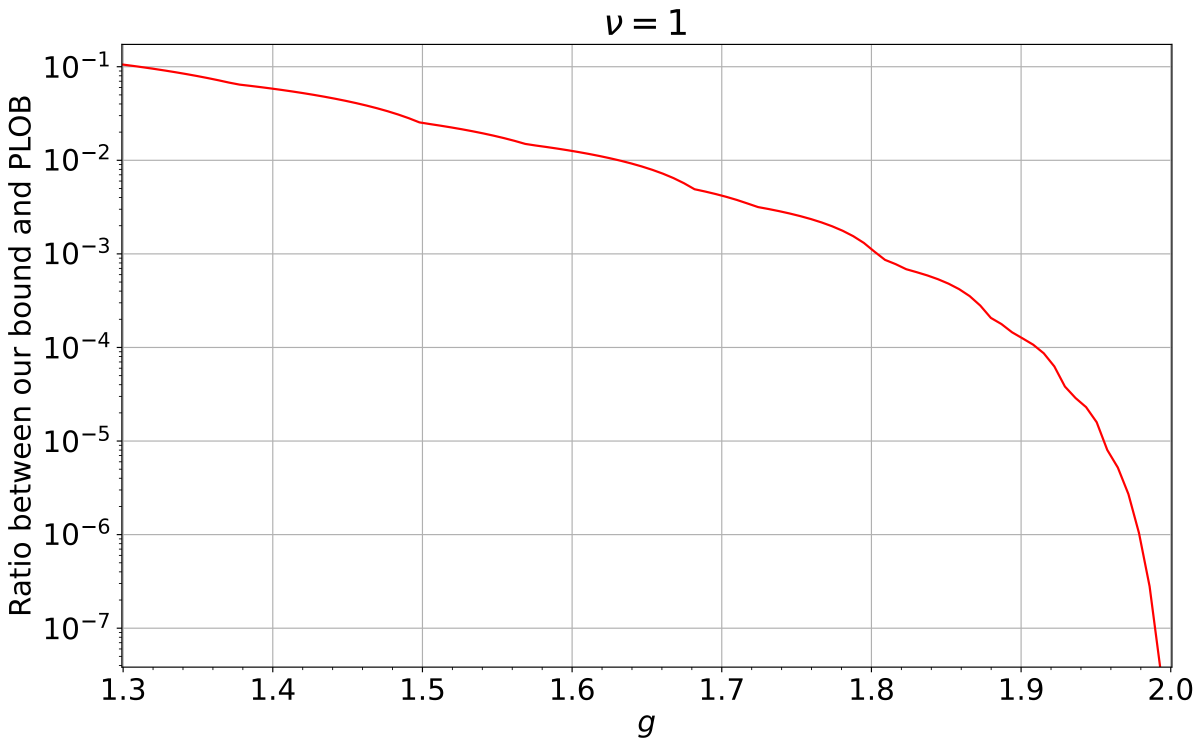


FIG. 10. Ratio between our new lower bound on the two-way capacities of the thermal amplifier $\Phi_{g,\nu}$ in (S244) and the PLOB bound in (S49) as a function of g for $\nu = 1$.

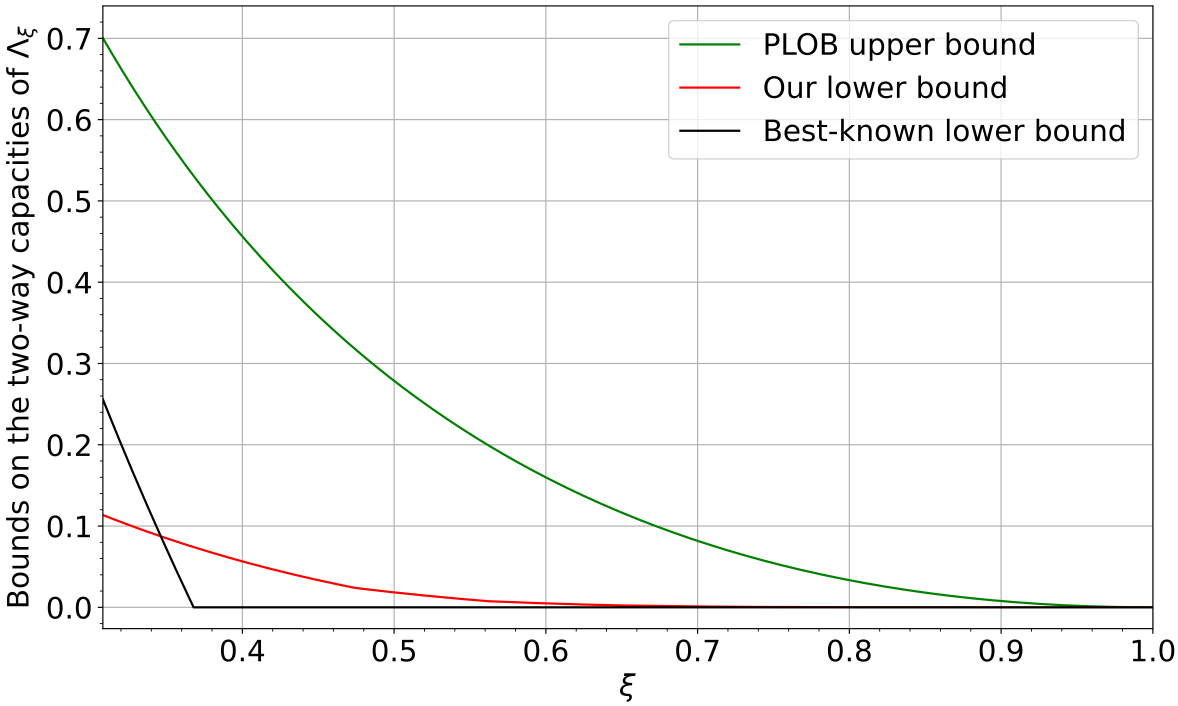


FIG. 11. Bounds on the two-way quantum capacity $Q_2(\Lambda_\xi)$ and secret-key capacity $K(\Lambda_\xi)$ of the additive Gaussian noise plotted with respect to ξ. The red line is our new lower bound obtained by exploiting (S246). The black line is the best known lower bound on $Q_2(\Lambda_\xi)$, which is the coherent information lower bound reported in (S62). The green line is the PLOB bound reported in (S61).