Finite-resource teleportation stretching for continuous-variable systems

Riccardo Laurenza, Samuel L. Braunstein, and Stefano Pirandola
Computer Science and York Centre for Quantum Technologies,
University of York, York YO10 5GH, United Kingdom

We show how adaptive protocols of quantum and private communication through bosonic Gaussian channels can be simplified into much easier block versions that involve resource states with finite energy. This is achieved by combining the adaptive-to-block reduction technique devised in [Pirandola et al., arXiv:1510.08863], based on teleportation stretching and relative entropy of entanglement, with the simulation of Gaussian channels introduced by [Liuzzo-Scorpo et al., arXiv:1705.03017]. In this way, we derive weak converse upper bounds for the secret-key capacity of phase-insensitive Gaussian channels, which closely approximate the optimal limit for infinite energy. Our results apply to both point-to-point and repeater-assisted private communications.

I. INTRODUCTION

Establishing the ultimate limits of quantum and private communications is important [1, 2], not only to explore the boundary of quantum mechanics but also to provide benchmarks for testing the practical performance of experimental and technological implementations. This problem is important for quantum systems of any dimension [3, 4] and, in particular, for infinite-dimensional ones, also known as continuous-variable (CV) systems [5–8]. In quantum information and quantum optics, the most important CV systems are the bosonic modes of the electromagnetic field [6], which are typically used at the optical or telecom wavelengths. In any protocol of quantum communication, such modes are subject to loss and noise, and the most typical and basic model for such kind of decoherence is the single-mode Gaussian channel.

It is known that protocol of private communication and quantum key distribution (QKD) are limited in both rate and distance due to decoherence, no matter if the communication line is a free-space link or a fiber connection. This limitation is perhaps best simplified by the rate-loss scaling of ideal single-photon BB84 protocol [9] whose optimal rate scales as $\eta/2$ secret bits per channel use, where η is the transmissivity of the channel. Recently, this fundamental rate-loss limit has been fully characterized. By optimizing over the most general protocols for key generation over a lossy channel, Ref. [10] established its secret-key capacity to be $K(\eta) = -\log_2(1-\eta)$ which is about 1.44η secret bits per channel use at long distances ($\eta \simeq 0$). This result sets a general benchmark for quantum repeaters [11–33] and completes a long-standing investigation started back in 2009 [34, 35], with the discovery of the best known lower bound.

The main technique that led to establish the previous capacity is based on a suitable combination of two ingredients, the relative entropy of entanglement (REE) [36–38] suitable extended from states to channels (using results from Refs. [39–41]), and teleportation stretching, which reduces any adaptive (feedback-assisted) quantum protocol over an arbitrary channel into a much simpler block version. This latter technique is a full extension and generalization of previous approaches [42–45] that only worked for specific classes of channels and were designed to reduce quantum error correcting code (QECC) protocols into entanglement distillation. Without doubts, the generalization to an arbitrary task over an arbitrary quantum channel has been one of the key insights of Ref. [10], and this has been widely exploited in recent literature, with a number of follow-up papers in the area of quantum Shannon theory [4] (e.g., on strong converse rates, broadcast capacities etc.)

The core of teleportation stretching is the idea of channel simulation, where an arbitrary quantum channel is replaced by local operations and classical communication (LOCC) applied to the input and a suitable resource state [10, 54]. This powerful idea is rooted in the protocol of teleportation [46, 47] and first proposed in Ref. [42], despite originally limited to the simulation of Pauli channels [48] (see also Ref. [49]). Later, this core idea was extended to generalized teleportation protocols [44, 50] and CV teleportation [51] in Refs. [43, 45]. The final and more general form involves a simulation via arbitrary LOCCs, as formulated in Ref. [10]. In particular, the simulation of bosonic channels is typically asymptotic, which means that they need a suitable limit over sequences of resource states, which comes from the fact that the Choi matrices of such channels are asymptotic states [10].

Here we consider a different type of simulation for bosonic Gaussian channels, which is based on finite-energy two-mode Gaussian states as recently introduced in Ref. [52]. We use this particular simulation at the core of teleportation stretching in order to simplify adaptive protocols. Not only this represents an interesting novel design (with potential applications beyond this work) but also allows us to derive upper bounds for the secret-key capacities of phase-insensitive Gaussian channels which well approximate the asymptotic results of Ref. [10].

The paper is organized as follows. In Sec. II, we review the tool of channel simulation. In Sec. III we use this tool with teleportation stretching, deriving a new single-letter bound for single-mode Gaussian channels. This bound is explicitly computed in Sec. IV, where it is also compared with the infinite-energy one of Ref. [10]. Theory is then extended to chain of quantum repeaters in Sec. V. Finally, Sec. VI is for conclusions.

II. SIMULATION OF BOSONIC CHANNELS

A. Preliminaries

As discussed in Ref. [10] an arbitrary quantum channel $\mathcal{E}$ can be simulated by a trace-preserving LOCC $\mathcal{T}$ and a suitable resource state σ, i.e.

$$\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \sigma) \ . \tag{1}$$

A channel is called σ-stretchable if it has σ as a resource state via some LOCC simulation as in Eq. (1). An important case is when the channel is Choi-stretchable, which means that the resource state can be chosen to be its Choi matrix $\sigma = \rho_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi)$, with Φ being a maximally entangled state. For a bosonic channel, the maximally entangled state is an EPR state with infinite energy, so that the Choi matrix of a bosonic channel is energy-unbounded. For this reason one has to work with a sequence of two-mode squeezed vacuum (TMSV) states [5] Φ^μ with variance $\mu = \bar{n} + 1/2$, where $\bar{n}$ is the average number of thermal photons in each mode. By definition, the EPR state is defined as $\Phi := \lim_\mu \Phi^\mu$ and the Choi matrix of a bosonic channel $\mathcal{E}$ is defined by

$$\rho_{\mathcal{E}} := \lim_\mu \rho^\mu_{\mathcal{E}}, \quad \rho^\mu_{\mathcal{E}} = \mathcal{I} \otimes \mathcal{E}(\Phi^\mu) \ . \tag{2}$$

This means that the simulation needs to be asymptotic, i.e., of the type

$$\mathcal{E}(\rho) = \lim_\mu \mathcal{T}(\rho \otimes \rho^\mu_{\mathcal{E}}) \ . \tag{3}$$

Ref. [10] identified a simple sufficient condition for a quantum channel to be Choi-stretchable, even asymptotically as in Eq. (3): teleportation covariance. In the bosonic case, a channel $\mathcal{E}$ is teleportation-covariant if, for any random displacement D (as induced by CV teleportation [47, 51]), we may write

$$\mathcal{E}(D\rho D^\dagger) = V\mathcal{E}(\rho)V^\dagger, \tag{4}$$

for some unitary V. It is clear that bosonic Gaussian channels are teleportation covariant and, therefore, Choi-stretchable, with asymptotic simulation as in Eq. (3).

B. Simulation of Gaussian channels with finite-energy resource states

Recently, Ref. [52] has shown that all single-mode phase-insensitive Gaussian channels can be simulated by applying CV teleportation to a particular class of Gaussian states as resource. Consider a single-mode Gaussian state with mean value $\bar{x}$ and covariance matrix (CM) $\mathbf{V}$ [5]. The action of a single-mode Gaussian channel can be expressed in terms of the statistical moments as follows

$$\bar{x} \to \mathbf{T}\bar{x}, \quad \mathbf{V} \to \mathbf{T}\mathbf{V}\mathbf{T}^T + \mathbf{N}, \tag{5}$$

where $\mathbf{T}$ and $\mathbf{N} = \mathbf{N}^T$ are 2×2 real matrices satisfying the conditions [5]

$$\mathbf{N} = \mathbf{N}^T \geq 0 \ , \quad \det \mathbf{N} \geq (\det \mathbf{T} - 1)^2. \tag{6}$$

In particular, the previous channel is called phase-insensitive if the two matrices take the specific diagonal forms

$$\mathbf{T} = \sqrt{\eta}\mathbf{I}, \quad \mathbf{N} = \nu\mathbf{I} \tag{7}$$

where $\eta \in \mathbb{R}$ is a transmissivity parameter, while $\nu \geq 0$ represents added noise.

According to Ref. [52], a phase-insensitive Gaussian channel $\mathcal{E}_{\eta,\nu}$ can be simulated as follows

$$\mathcal{E}_{\eta,\nu}(\rho) = \mathcal{T}_\eta(\rho \otimes \sigma_\nu), \tag{8}$$

where $\mathcal{T}_\eta$ is the Braunstein-Kimble protocol with gain $\sqrt{\eta}$ [51, 53], and σ_ν is a zero-mean two-mode Gaussian state with CM

$$\mathbf{V}(\sigma_\nu) = \begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I} \end{pmatrix}, \tag{9}$$

where [52]

$$\begin{aligned} a &= \frac{e^{2r} - 1 + \eta(1 + e^{-2r})}{e^{2r}(\eta - 1) + \eta + 1}, \quad b = e^{-2r} + (1 + a)\tanh r, \\ c &= e^{-2r}[(1 + a)(e^{2r}a - 1)\tanh r]^{1/2}, \end{aligned} \tag{10}$$

and the entanglement parameter $r \geq 0$ is connected to the channel parameter via the relation

$$\nu = e^{-2r}(\eta + 1). \tag{11}$$

III. FINITE-RESOURCE TELEPORTATION STRETCHING OF AN ADAPTIVE PROTOCOL

Here we plug the previous finite-resource simulation into the tool of teleportation stretching. We start by providing some necessary definitions on adaptive protocols and secret-key capacity. Then, we review a general upper bound (weak converse) based on the REE. Finally, following the recipe of Ref. [10, 54] we show how to use the finite-resource simulation to simplify an adaptive protocol and reduce the REE bound to a single-letter quantity.

A. Adaptive protocols and secret-key capacity

The most general protocol for key generation is based on adaptive LOCCs, i.e., local operations assisted by unlimited and two-way classical communication. Each transmission through the quantum channel is interleaved by two of such LOCCs. The general formalism can be found in Ref. [10] and goes as follows. Assume that two remote users, Alice and Bob, have two local registers of quantum systems (modes), $\mathbf{a}$ and $\mathbf{b}$, which are in some fundamental state $\rho_{\mathbf{a}} \otimes \rho_{\mathbf{b}}$. The two parties applies an adaptive LOCC Λ_0 before the first transmission.

In the first use of the channel, Alice picks a mode a_1 from her register $\mathbf{a}$ and sends it through the channel $\mathcal{E}$. Bob gets the output mode b_1 which is included in his local register $\mathbf{b}$. The parties apply another adaptive LOCC Λ_1. Then, there is the second transmission and so on. After n uses, we have a sequence of LOCCs $\{\Lambda_1, \Lambda_1, \ldots, \Lambda_n\}$ characterizing the protocol $\mathcal{L}$ and an output state $\rho^n_{\mathbf{ab}}$ which is ε-close to a target private state [56] with nR_n bits. Taking the limit of large n and optimizing over the protocols, we define the secret-key capacity of the channel

$$K(\mathcal{E}) = \sup_{\mathcal{L}} \lim_{n} R_n \ . \tag{12}$$

B. General upper bound

According to Theorem 1 (weak converse) in Ref. [10], a general upper bound for $K(\mathcal{E})$ is given in terms of the REE of the output state $\rho^n_{\mathbf{ab}}$

$$K(\mathcal{E}) \leq E_R^{\star}(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} \frac{E_R(\rho^n_{\mathbf{ab}})}{n} \ . \tag{13}$$

Recall that the REE of a state ρ is defined as $E_R(\rho) = \inf_{\sigma_{\text{sep}}} S(\rho||\sigma_{\text{sep}})$, where σ_{sep} is a separable state and the relative entropy is defined by $S(\rho||\sigma_{\text{sep}}) := \text{Tr}[\rho(\log_2 \rho - \log_2 \sigma_{\text{sep}})]$. These definitions can be easily adapted for asymptotic states of bosonic systems.

Note that the first and simplest proof of Eq. (13) can be found in Ref. [55] (second arxiv version of Ref. [10]). In order to avoid potential misunderstandings or misinterpretations of this proof, we report here the main points. For any protocol whose output $\rho^n_{\mathbf{ab}}$ is ε-close (in trace norm) to target private with rate R_n and dimension d, we may write

$$nR_n \leq E_R(\rho^n_{\mathbf{ab}}) + 4\varepsilon \log_2 d + 2H_2(\varepsilon), \tag{14}$$

where H_2 is the binary Shannon entropy. For distribution through a discrete variable (DV) channel, whose output is a DV state, we may write

$$\log_2 d \leq \alpha n R_n, \tag{15}$$

for some constant α (see also Eq. (21) of Ref. [55]). The exponential scaling in Eq. (15) comes from previous results in Refs. [40, 41]. The latter showed that, for any adaptive protocol with rate R_n, there is another protocol with the same asymptotic rate while having an exponential scaling for d.

The extension to a CV channel is achieved by a standard argument of truncation of the output Hilbert space. After the last LOCC Λ_n, Alice and Bob apply a truncation LOCC $\mathbb{T}_d$ which maps the output state $\rho^n_{\mathbf{ab}}$ into a truncated version $\rho^{n,d}_{\mathbf{ab}} = \mathbb{T}_d(\rho^n_{\mathbf{ab}})$ with total dimension d. The total protocol $\mathbb{T}_d \circ \mathcal{L} = \{\Lambda_0, \Lambda_1, \cdots, \Lambda_n, \mathbb{T}_d\}$ generates an output that is ε-close to a DV private state with $nR_{n,d}$ bits. Therefore, we may directly re-write Eq. (14) as

$$nR_{n,d} \leq E_R(\rho^{n,d}_{\mathbf{ab}}) + 4\varepsilon \log_2 d + 2H_2(\varepsilon). \tag{16}$$

Both the output and the target are DV states, so that we may again write Eq. (15) [57]. Because $\mathbb{T}_d$ is a trace-preserving LOCC, we exploit the monotonicity of the REE $E_R(\rho^{n,d}_{\mathbf{ab}}) \leq E_R(\rho^n_{\mathbf{ab}})$ and rewrite Eq. (16) as

$$R_{n,d} \leq \frac{E_R(\rho^n_{\mathbf{ab}}) + 2H_2(\varepsilon)}{n(1 - 4\alpha\varepsilon)} \ . \tag{17}$$

Taking the limit for large n and small ε (weak converse), this leads to

$$\lim_{n} R_{n,d} \leq \lim_{n} n^{-1} E_R(\rho^n_{\mathbf{ab}}). \tag{18}$$

The crucial observation is that in the right-hand side of the latter expression, there is no longer dependence on the truncation d. Therefore, in the optimization of $R_{n,d}$ over all protocols $\mathbb{T}_d \circ \mathcal{L}$ we can implicitly remove the truncation. Pedantically, we may write

$$\begin{aligned} K(\mathcal{E}) &= \sup_{d} \sup_{\mathbb{T}_d \circ \mathcal{L}} \lim_{n} R_{n,d} \\ &\leq \sup_{\mathcal{L}} \lim_{n} n^{-1} E_R(\rho^n_{\mathbf{ab}}) := E_R^{\star}(\mathcal{E}). \end{aligned} \tag{19}$$

Remark 1 *Note that the truncation argument was explicitly used in Ref. [55] to extend the bound to CV channels. See discussion after Eq. (23) of Ref. [55]. There a cut-off was introduced for the total CV Hilbert space at the output. Under this cutoff, the derivation for DV systems was repeated finding an upper bound which does not depend on the truncated dimension (this was done by using the monotonicity of the REE exactly as here). The cutoff was then relaxed in the final expression as above. The published version [10] includes other equivalent proofs but they have been just given for completeness.*

C. Simplification via teleportation stretching

One of the key insights of Ref. [10] has been the simplification of the general bound in Eq. (13) to a single-letter quantity. For bosonic Gaussian channels, this was achieved by using teleportation stretching with asymptotic simulations, where a channel is reproduced by CV teleportation over a sequence of Choi-approximating resource states. Here we repeat the procedure but adopting the finite-resource simulation of Ref. [52]. Recall that, more generally and differently from previous approaches [42–45], teleportation stretching does not reduce a protocol into entanglement distillation but maintains the task of the original protocol, so that adaptive key generation is reduced to block (non-adaptive) key generation.

Assume that the adaptive protocol is performed over a phase-insensitive Gaussian channel $\mathcal{E}_{\eta,\nu}$, so that we may use the simulation in Eq. (8), where $\mathcal{T}_\eta$ is the Braunstein-Kimble protocol with gain $\sqrt{\eta}$ and σ_ν is a zero-mean two-mode Gaussian state, specified by Eqs. (9)-(11). We may re-organize an adaptive protocol in such a way that each transmission through $\mathcal{E}_{\eta,\nu}$ is replaced by its resource state σ_ν. At the same time, each teleportation-LOCC $\mathcal{T}_\eta$ is included in the adaptive LOCCs of the protocol, which are all collapsed into a single LOCC $\bar{\Lambda}_\eta$ (trace-preserving after averaging over all measurements). In this way, we may decompose the output state $\rho^n_{\mathbf{ab}} := \rho_{\mathbf{ab}}(\mathcal{E}^{\otimes n}_{\eta,\nu})$ as

$$\rho^n_{\mathbf{ab}} := \bar{\Lambda}_\eta(\sigma_\nu^{\otimes n}) \ . \tag{20}$$

The computation of $E_R(\rho^n_{\mathbf{ab}})$ can now be remarkably simplified. In fact, we may write

$$\begin{aligned} E_R(\rho^n_{\mathbf{ab}}) &= \inf_{\sigma_{\rm sep}} S(\rho^n_{\mathbf{ab}}||\sigma_{\rm sep}) \\ &\overset{(1)}{\leq} \inf_{\bar{\Lambda}_\mu(\sigma_{\rm sep})} S[\bar{\Lambda}_\eta(\sigma_\nu^{\otimes n})||\bar{\Lambda}_\eta(\sigma_{\rm sep})] \\ &\overset{(2)}{\leq} \inf_{\sigma_{\rm sep}} S(\sigma_\nu^{\otimes n}||\sigma_{\rm sep}) = E_R(\sigma_\nu^{\otimes n}), \end{aligned} \tag{21}$$

where: (1) we consider the fact that $\bar{\Lambda}_\eta(\sigma_{\rm sep})$ form a subset of specific separable states, and (2) we use the monotonicity of the relative entropy under the trace-preserving LOCC $\bar{\Lambda}_\eta$. Therefore, by replacing in Eq. (13), we get rid of the optimization over the protocol (disappearing with $\bar{\Lambda}_\eta$) and we may write

$$K(\mathcal{E}_{\eta,\nu}) \leq \lim_n \frac{E_R(\sigma_\nu^{\otimes n})}{n} := E_R^\infty(\sigma_\nu) \leq E_R(\sigma_\nu) \ , \tag{22}$$

where we use the fact that the regularized REE is less than or equal the REE. Thus, we may write the following

Theorem 2 *Consider a phase-insensitive Gaussian channel $\mathcal{E}_{\eta,\nu}$, which is stretchable into a two-mode Gaussian state σ_ν as given in Eqs. (9)-(11). Its secret-key capacity must satisfy the bound*

$$K(\mathcal{E}_{\eta,\nu}) \leq E_R(\sigma_\nu) := \inf_{\sigma_{sep}} S(\sigma_\nu||\sigma_{sep}) \ . \tag{23}$$

Note that the new bound in Eq. (23) cannot beat the asymptotic bound established by Ref. [10] for bosonic channels, i.e.,

$$K(\mathcal{E}_{\eta,\nu}) \leq \inf_{\sigma^\mu_{\rm sep}} \liminf_{\mu\to+\infty} S(\rho^\mu_{\mathcal{E}_{\eta,\nu}}||\sigma^\mu_{\rm sep}), \tag{24}$$

where $\rho^\mu_{\mathcal{E}_{\eta,\nu}}$ is a Choi-approximating sequence as in Eq. (2), and $\sigma^\mu_{\rm sep}$ is an arbitrary sequence of separable states converging in trace norm. This can be seen from a quite simple argument [60]. In fact, according to Eqs. (2) and (8), we may write

$$\begin{aligned} \rho^\mu_{\mathcal{E}_{\eta,\nu}} &= \mathcal{I} \otimes \mathcal{E}_{\eta,\nu}(\Phi^\mu) \\ &= \mathcal{I} \otimes \mathcal{T}_\eta(\Phi^\mu \otimes \sigma_\nu) = \Delta(\sigma_\nu), \end{aligned} \tag{25}$$

where Δ is a trace-preserving LOCC. Therefore, $E_R(\rho^\mu_{\mathcal{E}_{\eta,\nu}}) \leq E_R(\sigma_\nu)$ and this relation is inherited by the bounds above. Notwithstanding this *no go* for the finite-resource simulation, we show that its performance is extremely good and well approximate the infinite-energy bounds found via Eq. (24).

IV. FINITE-RESOURCE BOUNDS FOR PHASE INSENSITIVE GAUSSIAN CHANNELS

We now proceed by computing the REE in Eq. (23) for the class of phase-insensitive single-mode channels. For this, we exploit the closed formula for the quantum relative entropy between Gaussian states which has been derived in Ref. [10] by using the Gibbs representation for Gaussian states [61]. Given two Gaussian states $\rho_1(u_1, V_1)$ and $\rho_2(u_2, V_2)$, with respective statistical moments u_i and V_i, their relative entropy is

$$S(\rho_1||\rho_2) = -\Sigma(V_1, V_1) + \Sigma(V_1, V_2) \ , \tag{26}$$

where we have defined

$$\Sigma(V_1, V_2) = \frac{\ln\det\left(V_2 + \frac{i\Omega}{2}\right) + \mathrm{Tr}(V_1 G_2) + \delta^T G_2 \delta}{2\ln 2} \tag{27}$$

with $\delta = u_1 - u_2$ and $G_2 = 2i\Omega \coth^{-1}(2iV_2\Omega)$ [61].

The computation of the REE involves an optimization over the set of separable states. Following the recipe of Ref. [10] we may construct a good candidate directly starting from the CM in Eq. (9). This separable state has CM with the same diagonal blocks as in Eq. (9), but where the off-diagonal term is replaced as follows

$$c \to c_{\rm sep} := \sqrt{(a - 1/2)(b - 1/2)} \ . \tag{28}$$

By using this separable state $\tilde{\sigma}_{\rm sep}$ we may write the further upper bound

$$E_R(\sigma_\nu) \leq \Psi(\mathcal{E}) := S(\sigma_\nu||\sigma^{\rm opt}_{\rm sep}). \tag{29}$$

In the following, we compute this bound for the various types of phase-insensitive channels.

A. Thermal-loss channel

This channel can be modelled as a beam splitter of transmissivity η where the input signals are combined with a thermal environment such that the quadratures transform according to $\hat{\mathbf{x}} \to \sqrt{\eta}\hat{\mathbf{x}} + \sqrt{1-\eta}\hat{\mathbf{x}}_{th}$, where $\hat{\mathbf{x}}_{th}$ are in a thermal state with $\bar{n}$ photons. In terms of the statistical moments, the action of the thermal-loss channel $\mathcal{E}_{\eta,\bar{n}}$ can be described by the matrices in Eq. (7) with parameter $\nu = (1-\eta)(\bar{n}+1/2)$. This means that the squeezing parameter r of the resource state now reads

$$r = \frac{1}{2}\log\left[\frac{\eta+1}{\left(\bar{n}+\frac{1}{2}\right)(1-\eta)}\right] \ . \tag{30}$$

By combining this relation with the ones in Eq. (10) and computing the relative entropy, we find [63] the finite-resource bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ which is plotted in Fig. 1 and therein compared with the infinite-energy bound $\Phi(\mathcal{E}_{\eta,\bar{n}})$ derived of Ref. [10]. The latter is given by [10]

$$\Phi(\mathcal{E}_{\eta,\bar{n}}) = -\log_2[(1-\eta)\eta^{\bar{n}}] - h(\bar{n}), \tag{31}$$

for $\bar{n} < \eta/(1-\eta)$ and zero otherwise, and we set $h(x) := (x+1)\log_2(x+1) - x\log_2 x$. It is clear that we have

$$K(\mathcal{E}_{\eta,\bar{n}}) \leq \Phi(\mathcal{E}_{\eta,\bar{n}}) \leq \Psi(\mathcal{E}_{\eta,\bar{n}}), \tag{32}$$

but the two bounds are exceptionally close, especially at high and low transmissivities.

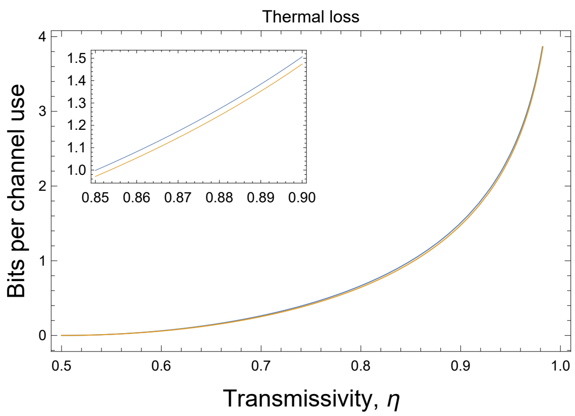

FIG. 1: Finite-resource bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ on the secret-key capacity of the thermal loss channel (light blue curve) as a function of the transmissivity η, compared with the infinite-energy bound $\Phi(\mathcal{E}_{\eta,\bar{n}})$ (orange curve) derived in Ref. [10]. The two curves are plotted for $\bar{n} = 1$ thermal photons.

B. Amplifier channel

This channel is described by $\hat{x} \to \sqrt{\eta}\hat{\mathbf{x}} + \sqrt{\eta - 1}\hat{\mathbf{x}}_{th}$, where $\eta > 1$ is the gain and $\hat{\mathbf{x}}_{th}$ is in a thermal state with $\bar{n}$ photons. This channel $\mathcal{E}_{\eta,\bar{n}}$ is described by the matrices in Eq. (7) with parameter $\nu = (\eta-1)(\bar{n}+1/2)$. By repeating the previous calculations, we find [63] the finite-resource bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ plotted in Fig. 2 and where it is compared with the infinite-energy bound [10]

$$\Phi(\mathcal{E}_{\eta,\bar{n}}) = -\log_2\left(\frac{\eta^{\bar{n}+1}}{\eta-1}\right) - h(\bar{n}), \tag{33}$$

for $\bar{n} < (\eta-1)^{-1}$ and zero otherwise. Approximation is very good, especially at low and high gains.

C. Additive-noise Gaussian channel

Another important channel is represented by the additive-noise Gaussian channel, which is the simplest

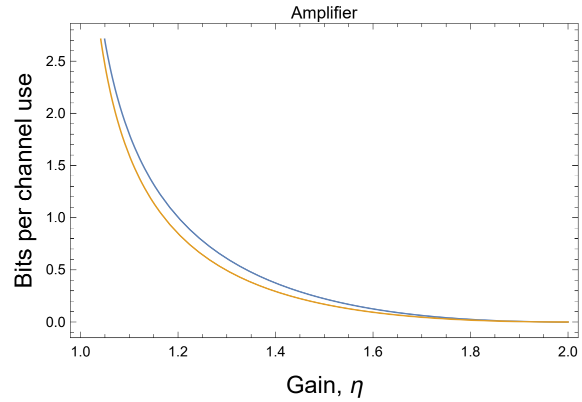

FIG. 2: Finite-resource bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ on the secret-key capacity of the amplifier channel (light blue curve) as a function of the gain η, compared with the optimal bound for infinite energy $\Phi(\mathcal{E}_{\eta,\bar{n}})$ (orange curve). The two curves are plotted for $\bar{n} = 1$ thermal photons.

model of bosonic decoherence. In terms of the input-output transformations, the quadratures transforms according to $\hat{\mathbf{x}} \to \hat{\mathbf{x}} + (z,z)^T$ where z is a classical Gaussian variable with zero mean and variance $\xi \geq 0$. This channel $\mathcal{E}_\xi$ is described by the matrices in Eq. (7) with $\eta = 1$ and $\nu = \xi$. The finite-resource bound [63] $\Psi(\mathcal{E}_\xi)$ on the secret key capacity is plotted in Fig. 3 and compared with the infinite-energy bound [10]

$$\Phi(\mathcal{E}_\xi) = \frac{\xi - 1}{\ln 2} - \log_2 \xi, \tag{34}$$

for $\xi < 1$, while zero otherwise. As we can see the approximation is again excellent over all the range.

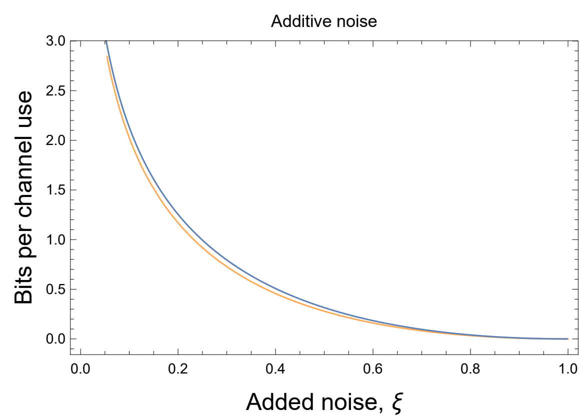

FIG. 3: Finite-resource bound $\Psi(\mathcal{E}_\xi)$ on the secret-key capacity of the additive noise channel (light blue curve) as a function of the added noise ξ, compared with the optimal bound for infinite energy $\Phi(\mathcal{E}_\xi)$ (orange curve).

D. Pure-loss channel

For the pure-loss channel, the upper bound derived in the limit of infinite energy [10] coincides with the lower bound computed with the reverse coherent information [34, 35]. This means that we are able to fully characterize the secret-key capacity for this specific bosonic channel. This is also known as the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [10]

$$\mathcal{K}(\eta) = -\log_2(1-\eta) \simeq 1.44\eta \text{ for } \eta \simeq 0 \ , \quad (35)$$

and provides the fundamental rate-loss scaling of long-distance repeaterless optical communications.

Consider now the finite-resource teleportation simulation of a pure-loss channel. It is easy to check that we cannot use the parametrization in Eq. (10). In fact, for a pure-loss channel, we have $\nu = 1-\eta$ so that Eq. (11) provides $e^{2r} = (1+\eta)/(1-\eta)$. Replacing the latter in Eq. (10), we easily see that we have divergences (e.g., the denominator of a becomes zero). For the pure loss channel, we therefore use a different simulation, where the resource state is a two-mode squeezed state with CM [62]

$$\sigma_\eta = \begin{pmatrix} a\mathbf{I} & \sqrt{a^2-1/4}\mathbf{Z} \\ \sqrt{a^2-1/4}\mathbf{Z} & a\mathbf{I} \end{pmatrix}, \ a = \frac{\eta+1}{2(1-\eta)} \ . \quad (36)$$

By exploiting this resource state, we derive [63] the bound $\Psi(\mathcal{E}_\eta)$ shown in Fig. 4, where it is compared with the secret-key capacity $K(\eta)$. We can see that, in this case, the approximation is not very good.

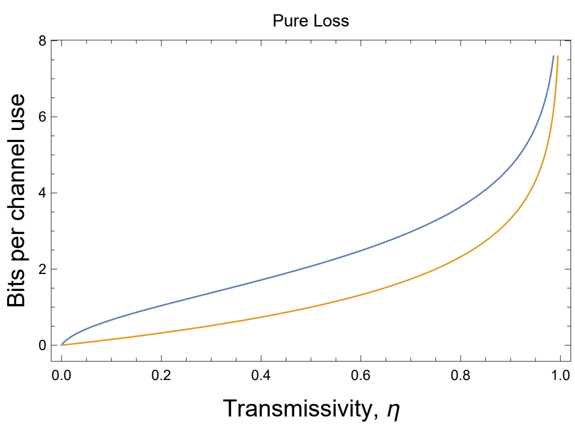

FIG. 4: Finite-resource bound $\Psi(\mathcal{E}_\eta)$ on the secret-key capacity of the pure-loss channel (light blue curve) as a function of the transmissivity η, compared with its secret key capacity or PLOB bound $K(\eta) = -\log_2(1-\eta)$ (orange curve).

V. EXTENSION TO REPEATER-ASSISTED PRIVATE COMMUNICATION

Here we extend the previous treatment to repeater-assisted private communication. We consider the basic scenario where Alice $\mathbf{a}$ and Bob $\mathbf{b}$ are connected by a chain of N quantum repeaters $\{\mathbf{r}_1, \ldots, \mathbf{r}_N\}$, so that there are a total of $N+1$ quantum channels $\{\mathcal{E}_i\}$ between them. Assume that these are phase-insensitive Gaussian channels $\mathcal{E}_i := \mathcal{E}_{\eta_i,\nu_i}$ with parameters (η_i, ν_i). The most general adaptive protocol for key distribution through the chain is described in Ref. [59] and goes as follows.

Alice, Bob and all the repeaters prepare their local registers $\{\mathbf{a}, \mathbf{r}_1, \ldots, \mathbf{r}_N, \mathbf{b}\}$ into a global initial state ρ^0 by means of a network LOCC Λ_0, where each node in the chain applies LOs assisted by unlimited and two-way CCs with all the other nodes. In the first transmission, Alice pick a system $a_1 \in \mathbf{a}$ and sends it to the first repeater; after another network LOCC Λ_1, the first repeater communicates with the second repeater; then there is another network LOCC Λ_2 and so on, until Bob is eventually reached, which terminates the fist use of the chain.

After n uses of the chain, we have a sequence of network LOCCs $\mathcal{L}$ defining the protocol and an output state $\rho^n_{\mathbf{ab}}$ for Alice and Bob which approximates some target private state with nR_n bits. By taking the limit for large n and optimizing over the protocols, we define the end-to-end or repeater-assisted secret-key capacity [59]

$$K(\{\mathcal{E}_i\}) = \sup_{\mathcal{L}} \lim_n R_n \ . \quad (37)$$

As shown in Ref. [59], we may extend the upper bound of Eq. (13). Then, we may use teleportation stretching and optimize over cuts of the chain, to simplify the bound to a single-letter quantity.

The network-reduction technique of Ref. [59] can be implemented by using the specific finite-resource simulation of Eq. (8), which leads to the following possible decompositions of the output state

$$\rho^n_{\mathbf{ab}} = \bar{\Lambda}_i(\sigma_{\nu_i}^{\otimes n}), \quad \text{for any } i = 1, \ldots, N, \quad (38)$$

where $\bar{\Lambda}_i$ is a trace-preserving LOCC and σ_{ν_i} is the resource state associated with the ith Gaussian channel. By repeating the derivation of Ref. [59], this leads to

$$K(\{\mathcal{E}_i\}) \leq \min_i E_R(\sigma_{\nu_i}) \leq \min_i S(\sigma_{\nu_i}||\sigma^{\text{opt}}_{i,\text{sep}}) := \Psi(\{\mathcal{E}_i\}) \ , \quad (39)$$

where Ψ is the upper bound coming from our choice of the separable state $\sigma^{\text{opt}}_{i,\text{sep}}$ in the REE. This upper bound needs to be compared with the one $\Phi(\{\mathcal{E}_i\})$ obtained in the limit of infinite energy [59].

As an example consider an additive-noise Gaussian channel with noise variance ξ. Let us split the communication line by using N "equidistant" repeaters [64], in such a way that each link is an additive-noise Gaussian channel $\mathcal{E}_i$ with the same variance $\xi_i = \xi/(N+1)$. From Eq. (39), we derive

$$\Psi(\{\mathcal{E}_i\}) = \Psi(\mathcal{E}_{\xi/(N+1)}), \quad (40)$$

which is plotted in Fig. 5 and compared with the corresponding infinite-energy bound. As we can see the approximation is extremely good.

Similarly, consider a fiber connection with total transmissivity η, so that the insertion of N equidistant repeaters [64] creates $N+1$ pure-loss channels, each with transmissivity $\eta_i = \sqrt[N+1]{\eta}$. From Eq. (39), we find

$$\Psi(\{\mathcal{E}_i\}) = \Psi(\mathcal{E}_{\sqrt[N+1]{\eta}}), \quad (41)$$

which is plotted in Fig. 6 and compared with the infinite-energy bound, with not so good approximation.

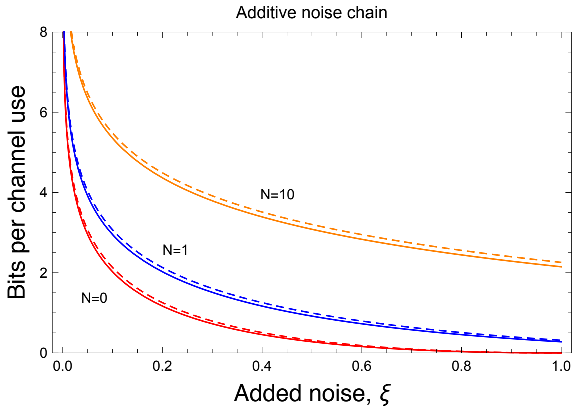

FIG. 5: Secret-key capacity of a chain of N equidistant repeaters creating $N+1$ additive-noise Gaussian channels with variances $\xi_i = \xi/(N+1)$. We compare the finite-resource bound (dashed) with the infinite-energy bound (solid) for different values of N as a function of the overall added noise of the chain ξ.

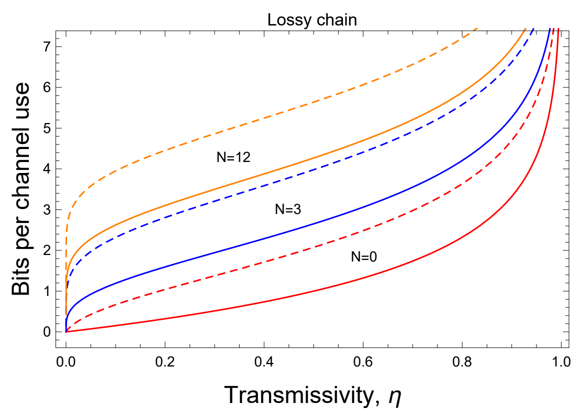

FIG. 6: Secret-key capacity of a chain of N equidistant repeaters creating $N+1$ pure-loss channels with transmissivities $\eta_i = \sqrt[N+1]{\eta}$. We compare the finite-resource bound (dashed) with the infinite-energy bound (solid) for different values of N as a function of the overall transmissivity of the chain η.

VI. CONCLUSION

In this work we have presented a novel design for the technique of teleportation stretching [10] for single-mode bosonic Gaussian channels, where the core channel simulation [52] is based on a finite-energy two-mode Gaussian state processed by the Braunstein-Kimble protocol [51] with suitable gains. Such an approach removes the need of using an asymptotic simulation where the sequence of states approximates the energy-unbounded Choi matrix of a Gaussian channel, even though the infinite energy limit remains at the level of Alice's quantum measurement which is ideally a CV Bell detection (i.e., a projection onto displaced Einstein-Podolsky-Rosen states).

By using this approach we compute the weak converse bound for the secret key capacity of all phase-insensitive single-mode Gaussian channels, which include the thermal-loss channel, the quantum amplifier and the additive-noise Gaussian channel. With the exception of the pure-loss channel, we show that the bounds so derived are very close to the tightest known bound established in Ref. [10] by using asymptotic Choi matrices. We checked that this is true not only for point-to-point private communication but also in repeater-assisted scenarios where Alice and Bob are connected by a chain of quantum repeaters. The tools developed here may have other applications; they may be applied to multi-point protocols [65] or to quantum metrology, e.g., to approximate the bounds for the adaptive estimation of Gaussian channels established in Ref. [66].

Acknowledgments. This work has been supported by the EPSRC via the 'UK Quantum Communications Hub' (EP/M013472/1). The authors would like to thank G. Adesso for feedback and comments on our first developments soon after the appearance of Ref. [52], and A. Mari for discussions about the relations between the various bounds, and the finite-resource simulation of the pure-loss channel The authors also thank valuable feedback from C. Lupo, G. Spedalieri, and C. Ottaviani.

[1] H. J. Kimble, Nature **453**, 1023 (2008).
[2] S. Pirandola and S. L. Braunstein, Nature **532**, 169 (2016).
[3] M. A. Nielsen, and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
[4] M. Hayashi, *Quantum Information Theory: Mathematical Foundation* (Springer-Verlag Berlin Heidelberg, 2017).
[5] C. Weedbrook *et al.,* Rev. Mod. Phys. **84**, 621 (2012).
[6] S. L. Braunstein, and P. Van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[7] A. Serafini, F. Illuminati, and S. De Siena, Journal of Physics B: Atomic, Molecular and Optical Physics **37**, L21 (2004).
[8] G. Adesso, S. Ragy, and A. R. Lee, Open Systems and Information Dynamics **21**, 1440001 (2014).
[9] C. H. Bennett, and G. Brassard, Proc. IEEE International Conf. on Computers, Systems, and Signal Processing, Bangalore, pp. 175–179 (1984).
[10] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017). See also arXiv:1510.08863 (2015).
[11] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932-5935 (1998).
[12] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
[13] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller,Nature (London) **414**, 413 (2001).
[14] Z. Zhao, T. Yang, Y.-A. Chen, A.-N. Zhang, and J.-W. Pan, Phys. Rev. Lett. **90**, 207901 (2003).
[15] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard,

H. Zbinden, and N. Gisin, Phys. Rev. Lett. **98**, 190503 (2007).

[16] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J.-W. Pan, Nature **454**, 1098-1101 (2008).

[17] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Phys. Rev. A **78**, 062319 (2008).

[18] R. Alleaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, New J. Phys. **11**, 075002 (2009).

[19] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).

[20] D. E. Bruschi, T. M. Barlow, M. Razavi, and A. Beige, Phys. Rev. A **90**, 032306 (2014).

[21] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014).

[22] K. Azuma, K. Tamaki, and W. J. Munro, Nature Comm. **6**, 10171 (2015).

[23] S. Bäuml, M. Christandl, K. Horodecki, and A. Winter, Nature Comm. **6**, 6908 (2015).

[24] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, Appl. Phys. B **122**, 96 (2016).

[25] J. Dias and T. C. Ralph, Phys. Rev. A **95**, 022312 (2017).

[26] M. Pant, H. Krovi, D. Englund, and S. Guha, Phys. Rev. A **95**, 012304 (2017).

[27] N. Lütkenhaus and S. Guha, *Quantum repeaters: Objectives, definitions and architectures*, available at http://wqrn.pratt.duke.edu/presentations, (2015).

[28] M. Christandl and A. Muller-Hermes, Communications in Mathematical Physics **353**, 821-852 (2017).

[29] F. Rozpedek, K. Goodenough, J. Ribeiro, N. Kalb, V. Caprara Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, *Realistic parameter regimes for a single sequential quantum repeater*, arXiv:1705.00043 (2017).

[30] N. Lo Piparo, N. Sinclair, and M. Razavi, *Memory-assisted quantum key distribution resilient against multiple-excitation effects*, arXiv:1707.07814 (2017).

[31] N. Lo Piparo, and M. Razavi, *Memory-assisted quantum key distribution immune to multiple-excitation effects*, Conference on Lasers and Electro-Optics (CLEO), 5-10 June 2016.

[32] N. Lo Piparo, M. Razavi, W. J. Munro, *Memory-Assisted Quantum Key Distribution with a Single Nitrogen Vacancy Center*, arXiv:1708.06532 (2017).

[33] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, *Routing entanglement in the quantum internet*, arXiv:1708.07142 (2017).

[34] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, Phys. Rev. Lett. **102**, 210501 (2009).

[35] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).

[36] V. Vedral, Rev. Mod. Phys. **74**, 197 (2002).

[37] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275-2279 (1997).

[38] V. Vedral, and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[39] B. Synak-Radtke and M. Horodecki, J. Phys. A: Math. Gen. **39**, L423-L437 (2006).

[40] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, Lecture Notes in Computer Science **4392**, 456-478 (2007). See also arXiv:quant-ph/0608199v3 for a more extended version.

[41] M. Christandl, N. Schuch, and A. Winter, Comm. Math. Phys. **311**, 397-422 (2012).

[42] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824-3851 (1996).

[43] J. Niset, J. Fiurasek, and N. J. Cerf, Phys. Rev. Lett. **102**, 120501 (2009).

[44] A. Muller-Hermes, *Transposition in quantum information theory* (Master's thesis, Technical University of Munich, 2012).

[45] M. M. Wolf, *Notes on "Quantum Channels & Operations"*, available at https://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/ Michael-Wolf/QChannelLecture.pdf (see page 36).

[46] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[47] S. Pirandola *et al.*, Nature Photon. **9**, 641-652 (2015).

[48] G. Bowen and S. Bose, Phys. Rev. Lett. **87**, 267901 (2001).

[49] T. P. W. Cope, L. Hetzel, L. Banchi, and S. Pirandola, Phys. Rev. A **96**, 022323 (2017).

[50] D. Leung and W. Matthews, IEEE Trans. Info. Theory **61**, 4486-4499 (2015).

[51] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869–872 (1998).

[52] P. Liuzzo-Scorpo, A. Mari, V. Giovannetti, and G. Adesso, *Optimal continuous variable quantum teleportation with limited resources*, arXiv:1705.03017 (2017).

[53] S. Pirandola, and S. Mancini, Laser Physics **16**, 1418 (2006).

[54] S. Pirandola and R. Laurenza, *General Benchmarks for Quantum Repeaters*, arXiv:1512.04945 (15 December 2015).

[55] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *The Ultimate Rate of Quantum Communications*, arXiv:1510.08863v2 (8 December 2015).

[56] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).

[57] Since the Hilbert space is finite-dimensional, the proof of Refs. [40, 41] automatically applies, i.e., the original protocol can be stopped after n_0 uses, and then repeated m times in an i.i.d. fashion, with $n = n_0 m$. Key distillitation applied to the m DV output copies implies a number of bits of CCs which is linear in m which, in turn, leads to an exponential scaling of d in n.

[58] C. Lupo and S. Pirandola, Phys. Rev. Lett. **117**, 190802 (2016).

[59] S. Pirandola, S. *Capacities of repeater-assisted quantum communications*, arXiv:1601.00966 (2016).

[60] Andrea Mari, private communication (15 May 2017).

[61] L. Banchi, S. L. Braunstein, and S. Pirandola, Phys. Rev. Lett. **115**, 260501 (2015).

[62] Andrea Mari, private communication (7 June 2017).

[63] The analitycal expression is too cumbersome to be reported here.

[64] It is easy to check that this is the optimal configuration for the repeaters.

[65] R. Laurenza, and S. Pirandola, Phys. Rev. A **96**, 032318 (2017).

[66] S. Pirandola, and C. Lupo, Phys. Rev. Lett. **118**, 100502 (2017).