Article:
Laurenza, Riccardo, Braunstein, Samuel L. orcid.org/0000-0003-4790-136X and Pirandola, Stefano orcid.org/0000-0001-6165-5615 (2018) Finite-resource teleportation stretching for continuous-variable systems. Scientific Reports. 15267. ISSN 2045-2322

https://doi.org/10.1038/s41598-018-33332-y

SCIENTIFIC REPORTS

OPEN

Finite-resource teleportation stretching for continuous-variable systems

Received: 23 July 2018
Accepted: 25 September 2018
Published online: 15 October 2018

Riccardo Laurenza, Samuel L. Braunstein & Stefano Pirandola

We show how adaptive protocols of quantum and private communication through bosonic Gaussian channels can be simplifed into much easier block versions that involve resource states with finite energy. This is achieved by combining an adaptive-to-block reduction technique devised earlier, based on teleportation stretching and relative entropy of entanglement, with a recent finite-resource simulation of Gaussian channels. In this way, we derive weak converse upper bounds for the secret-key capacity of phase-insensitive Gaussian channels which approximate the optimal limit for infinite energy. Our results apply to both point-to-point and repeater-assisted private communications.

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 protocols 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 key-generation protocols, Pirandola-Laurenza-Ottaviani-Banchi[10] have established the secret-key capacity of the lossy channel 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[11–24] and completes a long-standing investigation started back in 2009[25,26], when the best known lower bound was discovered.

The main technique that led to establishing the previous capacity is based on a suitable combination of two ingredients, the relative entropy of entanglement (REE)[27–29] suitably extended from states to channels (using results from refs[30–32]), 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[33–35] that only worked for specific classes of channels and were designed to reduce quantum error correcting code 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. See ref.[36] for a recent review on these topics and refs[36,37] for rigorous proofs of some related claims.

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]. This powerful idea is rooted in the protocol of teleportation[38,39] and first proposed in ref.[33], despite originally limited to the simulation of Pauli channels[40] (see also ref.[41]). Later, this core idea was extended to generalized teleportation protocols[35,42] and CV teleportation[43] in refs[34,44]. 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

Computer Science and York Centre for Quantum Technologies, University of York, York, YO10 5GH, United Kingdom. Correspondence and requests for materials should be addressed to S.P. (email: stefano.pirandola@york.ac.uk)

fact that the Choi matrices of such channels are asymptotic states[10]. Most importantly, such a simulation needs a careful control of the simulation error as first considered in ref.[10], otherwise technical divergences may appear in the results. This crucial aspect is discussed in detail in ref.[36], which also provides a direct comparison of the various simulation techniques appeared in the literature.

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.[45]. We use this particular simulation at the core of teleportation stretching in order to simplify adaptive protocols. This not only represents an interesting 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 approximate well the asymptotic results of ref.[10].

Results

Preliminaries on the simulation of bosonic channels. 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 $\sigma = \rho_{\mathcal{E}} := I \otimes \mathcal{E}(\Phi)$, with Φ being a maximally entangled state. For a bosonic channel, the maximally entangled state is an Einstein-Podolsky-Rosen (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 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

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

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

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

(More generally, one also needs to consider sequences of LOCCs $\mathcal{T}^{\mu}$, so that the asymptotic simulation reads $\mathcal{E}(\rho) = \lim_{\mu} \mathcal{T}^{\mu}(\rho \otimes \rho_{\mathcal{E}}^{\mu})$. For simplicity we omit this technicality, referring the reader to ref.[10] for more details.)

In ref.[10], we 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)[39,43], 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).

Simulation of Gaussian channels with finite-energy resource states. Recently, ref.[45] proposed a variant of Gaussian channel simulation[10], where single-mode phase-insensitive Gaussian channels are simulated by applying CV teleportation to a particular class of finite-energy Gaussian states as the 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

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

where $\mathbf{T}$ and $\mathbf{N} = \mathbf{N}^{T}$ are 2×2 real matrices satisfying suitable conditions[5]. In particular, the channel is called phase-insensitive if these two matrices take the specific diagonal forms

$$\mathbf{T} = \sqrt{\eta}\mathbf{I}, \ \ \mathbf{N} = \nu\mathbf{I} \tag{6}$$

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

According to ref.[45], a phase-insensitive Gaussian channel $\mathcal{E}_{\eta,\nu}$ can be simulated as follows

$$\mathcal{E}_{\eta,\nu}(\rho) = \mathcal{T}_{\eta}(\rho \otimes \sigma_{\nu}), \tag{7}$$

where $\mathcal{T}_{\eta}$ is the Braunstein-Kimble protocol with gain $\sqrt{\eta}$ [43,46], and σ_{ν} is a zero-mean two-mode Gaussian state with CM

$$\mathbf{V}(\sigma_{\nu}) = \begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I} \end{pmatrix}, \tag{8}$$

where[45]

$$a = \frac{2b + (\eta - 1)e^{-2r}}{2\eta}, \quad c = \frac{2b - e^{-2r}}{2\sqrt{\eta}}, \tag{9}$$

$$b = \frac{-|\eta - 1| + \eta e^{2r} + e^{-2r}}{2[\, -e^{2r}|\eta - 1| + \eta + 1]}, \tag{10}$$

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

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

Note that, with respect to the fomulas of ref.[45], we have an extra 1/2 factor in Eqs (8) and (11). This is due to the different notation we adopt here. We set the quadrature variance of the vacuum state to be 1/2, while it was equal to 1 in ref.[45]. Also note that, in the simulation of Eq. (7), one uses a Braunstein-Kimble protocol with an ideal CV Bell detection. The latter is an asymptotic measurement defined in the limit of infinite squeezing, i.e., infinite energy. For this reason, the finite-energy aspect of the simulation in Eq. (7) only refers to the resource state.

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 refs[10,47]. we show how to use the finite-resource simulation to simplify an adaptive protocol and reduce the REE bound to a single-letter quantity.

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), **a** and **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 **a** and sends it through the channel $\mathcal{E}$. Bob gets the output mode b_1 which is included in his local register **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 $\{\Lambda_0, \Lambda_1, \ldots, \Lambda_n\}$ characterizing the protocol $\mathcal{L}$ and an output state $\rho^n_{\mathbf{ab}}$ which is ε-close to a target private state[48] with nR_n bits. Taking the limit of large n and optimizing over the protocols, we define the secret-key capacity of the channel

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

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 $\rho^n_{\mathbf{ab}}$

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

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.[49] (the second arxiv version of ref.[10]). 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 state 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.[49]]. The exponential scaling in Eq. (15) comes from previous results in refs[31,32]. 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). In fact, since the Hilbert space is finite-dimensional, the proof of refs[31,32] automatically applies, i.e., the 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 distillation 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.

Because $\mathbb{T}_d$ is a trace-preserving LOCC, we exploit the monotonicity of the REE $E_R(\rho_{\mathbf{ab}}^{n,d}) \leq E_R(\rho_{\mathbf{ab}}^n)$ and rewrite Eq. (16) as

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

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

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

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

$$K(\mathcal{E}) = \sup_d \sup_{\mathbb{T}_d \circ \mathcal{L}} \lim_n R_{n,d} \leq \sup_{\mathcal{L}} \lim_n n^{-1} E_R(\rho_{\mathbf{ab}}^n) := E_R^*(\mathcal{E}). \tag{19}$$

Remark 1 *Note that the truncation argument was explicitly used in* ref.[49] *to extend the bound to CV channels. See discussion after* Eq. (23) *of* ref.[49]. *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.*

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 we adopt the finite-resource simulation of ref.[45]. Recall that, differently from previous approaches[33–35], 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. See ref.[36] for comparisons and clarifications.

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. (7), 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 (8–11). 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 $\overline{\Lambda}_\eta$ (trace-preserving after averaging over all measurements). In this way, we may decompose the output state $\rho_{\mathbf{ab}}^n := \rho_{\mathbf{ab}}(\mathcal{E}_{\eta,\nu}^{\otimes n})$ as

$$\rho_{\mathbf{ab}}^n = \overline{\Lambda}_\eta(\sigma_\nu^{\otimes n}). \tag{20}$$

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

$$E_R(\rho_{\mathbf{ab}}^n) = \inf_{\sigma_{\text{sep}}} S(\rho_{\mathbf{ab}}^n || \sigma_{\text{sep}}) \overset{(1)}{\leq} \inf_{\sigma_{\text{sep}}} S[\overline{\Lambda}_\eta(\sigma_\nu^{\otimes n}) || \overline{\Lambda}_\eta(\sigma_{\text{sep}})] \overset{(2)}{\leq} \inf_{\sigma_{\text{sep}}} S(\sigma_\nu^{\otimes n} || \sigma_{\text{sep}}) = E_R(\sigma_\nu^{\otimes n}), \tag{21}$$

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

Theorem 2 *Consider a phase-insensitive bosonic Gaussian channel $\mathcal{E}_{\eta,\nu}$, which is stretchable into a two-mode Gaussian state σ_ν as given in Eqs (8–11). Its secret-key capacity must satisfy the bound*

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

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

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

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[50]. In fact, according to Eqs (2) and (7), we may write

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

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 good and reasonably approximates the infinite-energy bounds that are found via Eq. (24).

Finite-resource bounds for phase insensitive Gaussian channels. We now proceed by computing the REE in Eq. (23) for the class of single-mode phase-insensitive Gaussian 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[51]. 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 $G_2 = 2i\Omega\,\mathrm{coth}^{-1}(2iV_2\Omega)$[51], where the matrix Ω is the symplectic form.

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. (8). This separable state has CM with the same diagonal blocks as in Eq. (8), 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

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

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

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 $\hat{\mathbf{x}}_{th}$ is 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. (6) with parameter $\nu = (1-\eta)(\bar{n} + 1/2)$. This means that the squeezing parameter r of the resource state now reads

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

By combining this relation with the ones in Eq. (10) and computing the relative entropy, we find 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 in 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 upper bounds are reasonably close.

Noisy amplifier channel. A noisy quantum amplifier is described by $\hat{\mathbf{x}} \to \sqrt{\eta}\hat{\mathbf{x}} + \sqrt{\eta-1}\hat{\mathbf{x}}_{th}$, 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. (6) with parameter $\nu = (\eta-1)(\bar{n}+1/2)$. By repeating the previous calculations, we find 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.

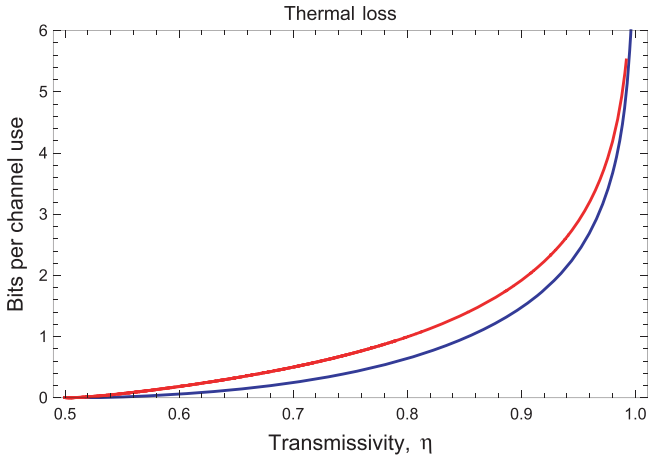

Figure 1. Finite-resource bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ on the secret-key capacity of the thermal loss channel (red upper curve) as a function of the transmissivity η, compared with the infinite-energy bound $\Phi(\mathcal{E}_{\eta,\bar{n}})$ (blue lower curve) derived in ref.[10]. The curves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

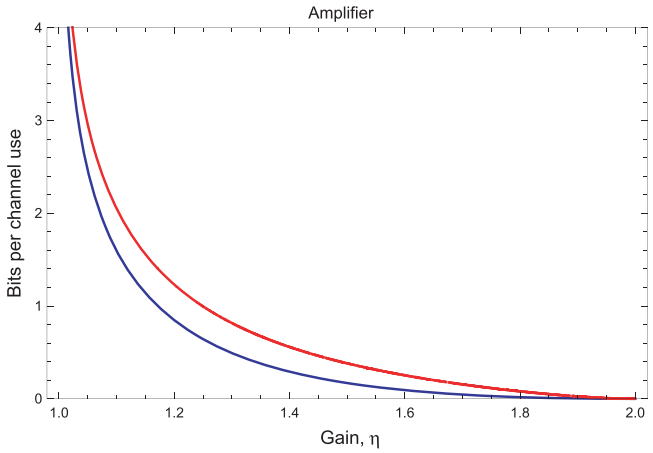

Figure 2. Finite-resource bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ on the secret-key capacity of the noisy amplifier channel (red upper curve) as a function of the gain η, compared with the optimal bound for infinite energy $\Phi(\mathcal{E}_{\eta,\bar{n}})$ (blue lower curve). The two curves are plotted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

Additive-noise Gaussian channel. Another important channel is represented by the additive-noise Gaussian channel, which is the simplest model of bosonic decoherence. In terms of the input-output transformations, the quadratures transforms according to $\hat{\mathbf{x}} \to \hat{\mathbf{x}} + (z, \quad z)^T$ 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. (6) with $\eta = 1$ and $\nu = \xi$. The finite-resource bound $\Psi(\mathcal{E}_\xi)$ 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.

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[25,26]. 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]

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

and fully characterizes the fundamental rate-loss scaling of point-to-point quantum 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 $\nu = (1 - \eta)/2$ 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

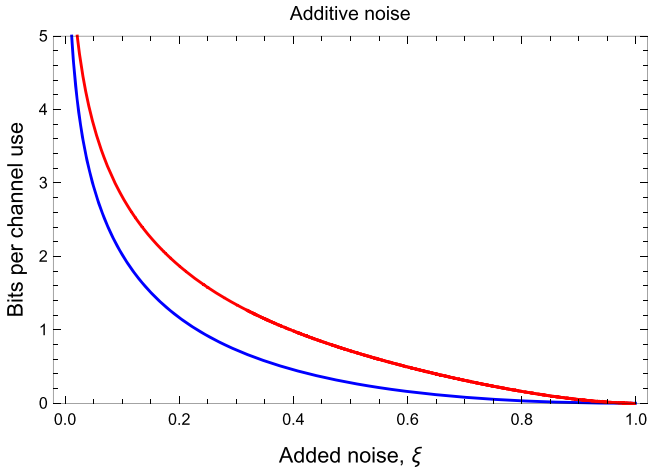

Figure 3. Finite-resource bound $\Psi(\mathcal{E}_\xi)$ on the secret-key capacity of the additive noise Gaussian channel (red upper curve) as a function of the added noise ξ, compared with the optimal bound for infinite energy $\Phi(\mathcal{E}_\xi)$ (blue lower curve).

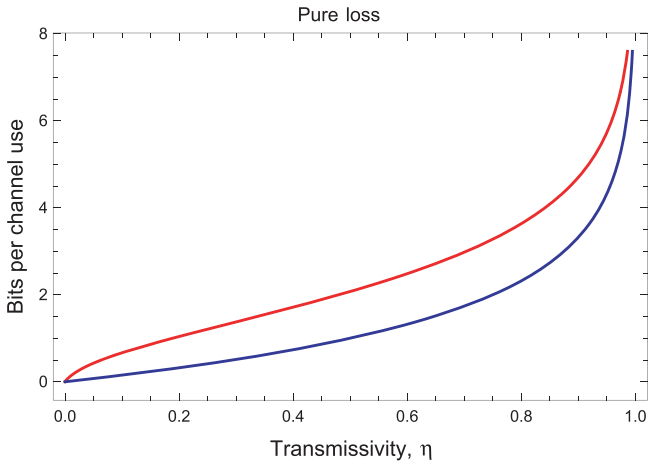

Figure 4. Finite-resource bound $\Psi(\mathcal{E}_\eta)$ on the secret-key capacity of the pure-loss channel (red upper curve) as a function of the transmissivity η, compared with its secret key capacity or PLOB bound $K(\eta) = -\log_2(1-\eta)$ (blue lower curve).

denominator of b 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[50]

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

By exploiting this resource state, we derive the bound $\Psi(\mathcal{E}_\eta)$ shown in Fig. 4, where it is compared with the secret-key capacity $K(\eta)$.

Extension to repeater-assisted private communication. Here we extend the previous treatment to repeater-assisted private communication. We consider the basic scenario where Alice **a** and Bob **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.[52] 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 picks 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 first use of the chain.

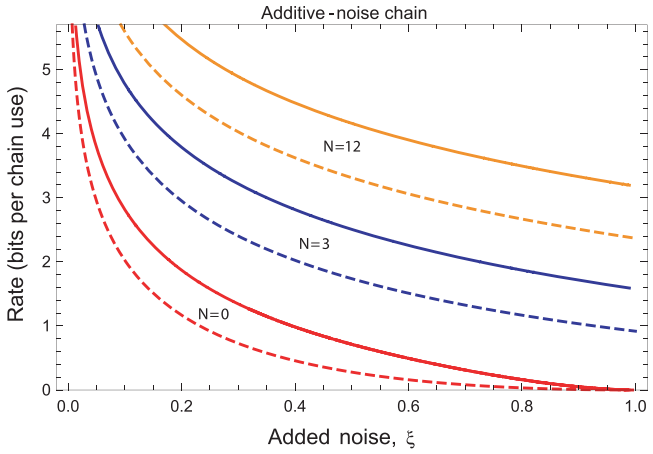

Figure 5. Secret-key capacity of a chain of N equidistant repeaters creating $N+1$ additive-noise Gaussian channels with variances $\xi_i = \xi/(N+1)$. We compare the finite-resource upper bound $\Psi(\{\mathcal{E}_i\})$ (solid lines) with the infinite-energy upper bound $\Phi(\{\mathcal{E}_i\})$ (dashed lines) for different values of N as a function of the overall added noise of the chain ξ.

After n uses of the chain, we have a sequence of network LOCCs $\mathcal{L}$ defining the protocol and an output state $\rho_{\mathbf{ab}}^n$ 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[52]

$$K(\{\mathcal{E}_i\}) = \sup_{\mathcal{L}} \lim_{n} R_n. \tag{37}$$

As shown in ref.[52], 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.[52] can be implemented by using the specific finite-resource simulation of Eq. (7), which leads to the following possible decompositions of the output state

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

where $\overline{\Lambda}_i$ 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.[52], this leads to

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

where Ψ is the upper bound coming from our choice of the separable state $\bar{\sigma}_{i,\text{sep}}$ in the REE. This upper bound needs to be compared with the one $\Phi(\{\mathcal{E}_i\})$ obtained in the limit of infinite energy[52]. As an example, consider an additive-noise Gaussian channel with noise variance ξ. Let us split the communication line by using N "equidistant" repeaters, in such a way that each link is an additive-noise Gaussian channel $\mathcal{E}_i$ with the same variance $\xi_i = \xi/(N+1)$. It is easy to check that this is the optimal configuration for the repeaters. From Eq. (39), we derive $\Psi(\{\mathcal{E}_i\}) = \Psi(\mathcal{E}_{\xi/(N+1)})$. This bound is plotted in Fig. 5 where we can se an acceptable approximation of the corresponding infinite-energy bound $\Phi(\{\mathcal{E}_i\})$.

Discussion

In this work we have presented a design for the technique of teleportation stretching[10] for single-mode bosonic Gaussian channels, where the core channel simulation[45] is based on a finite-energy two-mode Gaussian state processed by the Braunstein-Kimble protocol[43] with suitable gains. Such an approach removes the need for 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 EPR states). 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. We find that the bounds so derived are reasonably close to the tightest known bound established in ref.[10] by using asymptotic Choi matrices. We have considered not only for point-to-point communication but also a repeater-assisted scenario where Alice and Bob are connected by a chain of quantum repeaters.

The tools developed here may have other applications. For instance, they may be applied to multi-point protocols[53] and more complex quantum networks[52]. In an arbitrary multi-hop quantum communication network, the end-to-end capacities under single- and multi-path routing strategies may be expressed in terms of the REE of finite-energy resource states. In particular, these states can be identified by solving classical problems of network information theory (widest path or maximum flow) following the same approach in ref.[52]. In the context of quantum metrology, a finite-resource simulation (different from the one employed in the present paper) has

been recently exploited in ref.[54]. The stretching strategy adopted therein allows one to simplify the most general adaptive protocol for quantum parameter estimation into a block scheme, so that one can write an upper bound for the quantum Fisher information in terms of a finite-energy resource state. This allows one to lower-bound the minimum variance of the error that affects the adaptive estimation of noise parameters in Gaussian channels, with good approximation of the optimal bounds established in ref.[55] but based on asymptotic Choi matrices.

Note added. Our work first appeared on the arXiv in June 2017[56]. It has been revised after an imprecision in ref.[45] was fixed in ref.[57]. Independently and simultaneously, a related work[58] also built on the techniques of ref.[10], but its claims were restricted to a point-to-point thermal-loss channel in the non-asymptotic scenario.

Data Availability Statement

The datasets generated during the current study are available from the corresponding author on reasonable request.

References

1. Kimble, H. J. The quantum internet. *Nature* **453**, 1023 (2008).
2. Pirandola, S. & Braunstein, S. L. *Nature* **532**, 169 (2016).
3. Watrous, J. *The theory of quantum information* (Cambridge University Press, Cambridge, 2018).
4. Hayashi, M. *Quantum Information Theory: Mathematical Foundation* (Springer-Verlag Berlin Heidelberg, 2017).
5. Weedbrook, C. *et al*. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
6. Braunstein, S. L. & Van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513 (2005).
7. Serafini, A., Illuminati, F. & De Siena, S. Symplectic invariants, entropic measures and correlations of Gaussian states. *J. Phys. B* **37**, L21 (2004).
8. Adesso, G., Ragy, S. & Lee, A. R. Continuous variable quantum information: Gaussian states and beyond. *Open Syst. Inf. Dyn.* **21**, 1440001 (2014).
9. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Proc. IEEE International Conf. on Computers, Systems, and Signal Processing, Bangalore*, pp. 175–179 (1984).
10. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017). See also *Preprint arXiv*, 1510.08863 (Oct 2015).
11. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).
12. Dür, W., Briegel, H.-J., Cirac, J. I. & Zoller, P. Quantum repeaters based on entanglement purification. *Phys. Rev. A* **59**, 169 (1999).
13. Van Loock, P., Lütkenhaus, N., Munro, W. J. & Nemoto, K. Quantum repeaters using coherent-state communication. *Phys. Rev. A* **78**, 062319 (2008).
14. Alleaume, R., Roueff, F., Diamanti, E. & Lütkenhaus, N. QKD networks: topological optimization. *New J. Phys.* **11**, 075002 (2009).
15. Sangouard, N., Simon, C., de Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33 (2011).
16. Bruschi, D. E., Barlow, T. M., Razavi, M. & Beige, A. Repeat-until-success quantum repeaters. *Phys. Rev. A* **90**, 032306 (2014).
17. Muralidharan, S., Kim, J., Lütkenhaus, N., Lukin, M. D. & Jiang, L. Ultrafast and Fault-Tolerant Quantum Communication across Long Distances. *Phys. Rev. Lett.* **112**, 250501 (2014).
18. Dias, J. & Ralph, T. C. Quantum repeaters using continuous-variable teleportation. *Phys. Rev. A* **95**, 022312 (2017).
19. Pant, M., Krovi, H., Englund, D. & Guha, S. Rate-distance tradeoff and resource costs for all-optical quantum repeaters. *Phys. Rev. A* **95**, 012304 (2017).
20. Christandl, M. & Muller-Hermes, A. Relative Entropy Bounds on Quantum, Private and Repeater Capacities. *Commun. Math. Phys.* **353**, 821–852 (2017).
21. Rozpedek, F. *et al*. Parameter regimes for a single sequential quantum repeater. *Quantum Sci. Technol.* **3**, 034002 (2018).
22. Lo Piparo, N., Sinclair, N. & Razavi, M. Memory-assisted quantum key distribution resilient against multiple-excitation effects *Preprint arXiv*, 1707.07814 (July 2017).
23. Lo Piparo, N., Razavi, M. & Munro, W. J. Memory-Assisted Quantum Key Distribution with a Single Nitrogen-Vacancy Center. *Phys. Rev. A* **96**, 052313 (2017).
24. Pant, M. *et al*. Routing entanglement in the quantum internet. *Preprint arXiv*, 1708.07142 (Aug 2017).
25. Garca-Patrón, R., Pirandola, S., Lloyd, S. & Shapiro, J. H. Reverse coherent information. *Phys. Rev. Lett.* **102**, 210501 (2009).
26. Pirandola, S., Garca-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **102**, 050503 (2009).
27. Vedral, V. The role of relative entropy in quantum information theory. *Rev. Mod. Phys.* **74**, 197 (2002).
28. Vedral, V., Plenio, M. B., Rippin, M. A. & Knight, P. L. Quantifying Entanglement. *Phys. Rev. Lett.* **78**, 2275–2279 (1997).
29. Vedral, V. & Plenio, M. B. Entanglement Measures and Purification Procedures. *Phys. Rev. A* **57**, 1619 (1998).
30. Synak-Radtke, B. & Horodecki, M. J. On asymptotic continuity of functions of quantum states. *Phys. A: Math. Gen.* **39**, L423–L437 (2006).
31. Christandl, M. *et al* Unifying classical and quantum key distillation. *Proceedings of the 4th Theory of Cryptography Conference, Lecture Notes in Computer Scienc*e. **439**2, 456–478 See also *Preprint arXi*v, quant-ph/0608199v3 for a more extended version (2007).
32. Christandl, M., Schuch, N. & Winter, A. Entanglement of the antisymmetric state. *Comm. Math. Phys.* **311**, 397–422 (2012).
33. Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. & Wootters, W. K. Mixed State Entanglement and Quantum Error Correction. *Phys. Rev. A* **54**, 3824–3851 (1996).
34. Niset, J., Fiurasek, J. & Cerf, N. J. No-Go Theorem for Gaussian Quantum Error Correction. *Phys. Rev. Lett.* **102**, 120501 (2009).
35. Müller-Hermes, A. Master's thesis (Technical University of Munich, 2012).
36. Pirandola, S. *et al*. Theory of channel simulation and bounds for private communication. *Quantum Sci. Technol.* **3**, 035009 (2018).
37. Pirandola, S., Laurenza, R. & Braunstein, S. L. Teleportation simulation of bosonic Gaussian channels: Strong and uniform convergence. *Eur. Phys. J. D* **72**, 162 (2018). See also *Preprint arXiv*, 1712.01615 (2017).
38. Bennett, C. H. *et al*. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895 (1993).
39. Pirandola, S. *et al*. Advances in quantum teleportation. *Nature Photon.* **9**, 641–652 (2015).
40. Bowen, G. & Bose, S. Teleportation as a Depolarizing Quantum Channel, Relative Entropy, and Classical Capacity. *Phys. Rev. Lett.* **87**, 267901 (2001).
41. Cope, T. P. W., Hetzel, L., Banchi, L. & Pirandola, S. Simulation of non-Pauli channels. *Phys. Rev. A* **96**, 022323 (2017).
42. Leung, D. & Matthews, W. On the power of PPT-preserving and non-signalling codes. *IEEE Trans. Info. Theory* **61**, 4486–4499 (2015).
43. Braunstein, S. L. & Kimble, H. J. Teleportation of Continuous Quantum Variables. *Phys. Rev. Lett.* **80**, 869–872 (1998).

44. Giedke, G. & Cirac, J. I. The characterization of Gaussian operations and Distillation of Gaussian States. *Phys. Rev. A* **66**, 032316 (2002).
45. Liuzzo-Scorpo, P., Mari, A., Giovannetti, V. & Adesso, G. Optimal continuous variable quantum teleportation with limited resources. *Phys. Rev. Lett.* **119**, 120503 (2017).
46. Pirandola, S. & Mancini, S. Quantum Teleportation with Continuous Variables: a survey. *Laser Physics* **16**, 1418 (2006).
47. Pirandola, S. & Laurenza, R. General Benchmarks for Quantum Repeaters. *Preprint arXiv*, 1512.04945 (Dec 2015).
48. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. Secure key from bound entanglement. *Phys. Rev. Lett.* **94**, 160502 (2005).
49. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. The Ultimate Rate of Quantum Communications. *Preprint arXiv*, 1510.08863v2 (Dec 2015).
50. Mari, A. private communication (May and June 2017).
51. Banchi, L., Braunstein, S. L. & Pirandola, S. Quantum fidelity for arbitrary Gaussian states. *Phys. Rev. Lett.* **115**, 260501 (2015).
52. Pirandola, S. Capacities of repeater-assisted quantum communications. *Preprint arXiv*, 1601.00966 (Jan 2016).
53. Laurenza, R. & Pirandola, S. General bounds for sender-receiver capacities in multipoint quantum communications. *Phys. Rev. A* **96**, 032318 (2017).
54. Laurenza, R., Lupo, C., Spedalieri, G., Braunstein, S. L. & Pirandola, S. Channel Simulation in Quantum Metrology. *Quantum Meas. Quantum Metrol.* **5**, 1–12 (2018).
55. Pirandola, S. & Lupo, C. Ultimate Precision of Adaptive Noise Estimation. *Phys. Rev. Lett.* **118**, 100502 (2017).
56. Laurenza, R., Braunstein, S. L. & Pirandola, S. Finite-resource teleportation stretching for continuous-variable systems. *Preprint arXiv*, 1706.06065v1 (June 2017).
57. Liuzzo-Scorpo, P., Mari, A., Giovannetti, V. & Adesso, G. Erratum: Optimal Continuous Variable Quantum Teleportation with Limited Resources. *Phys. Rev. Lett.* **20**, 029904(E) (2018).
58. Kaur, E. & Wilde, M. M. Upper bounds on secret key agreement over lossy thermal bosonic channels. *Phys. Rev*. A **96**, 062318 (2017). See also *Preprint arX*iv, 1706.04590v1(June 2017).

Acknowledgements

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 comments on our first developments soon after the appearance of ref.[45], and A. Mari for discussions on the relations between the various bounds, and the finite-resource simulation of the pure-loss channel. The authors also thank C. Lupo, G. Spedalieri, C. Ottaviani, S. Tserkis, T. Ralph, and S. Lloyd.

Author Contributions

R.L. contributed to the theoretical derivations and found the finite-resource bounds. S.L.B. contributed to the general development of the ideas. S.P. developed the underlying theory and wrote the manuscript.

Additional Information

Competing Interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.