nature COMMUNICATIONS

ARTICLE

Received 15 Mar 2016 | Accepted 23 Feb 2017 | Published 26 Apr 2017

DOI: 10.1038/ncomms15043

OPEN

Fundamental limits of repeaterless quantum communications

Stefano Pirandola[1], Riccardo Laurenza[1], Carlo Ottaviani[1] & Leonardo Banchi[2]

Quantum communications promises reliable transmission of quantum information, efficient distribution of entanglement and generation of completely secure keys. For all these tasks, we need to determine the optimal point-to-point rates that are achievable by two remote parties at the ends of a quantum channel, without restrictions on their local operations and classical communication, which can be unlimited and two-way. These two-way assisted capacities represent the ultimate rates that are reachable without quantum repeaters. Here, by constructing an upper bound based on the relative entropy of entanglement and devising a dimension-independent technique dubbed 'teleportation stretching', we establish these capacities for many fundamental channels, namely bosonic lossy channels, quantum-limited amplifiers, dephasing and erasure channels in arbitrary dimension. In particular, we exactly determine the fundamental rate-loss tradeoff affecting any protocol of quantum key distribution. Our findings set the limits of point-to-point quantum communications and provide precise and general benchmarks for quantum repeaters.

[1] Department of Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK. [2] Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, UK. Correspondence and requests for materials should be addressed to S.P. (email: stefano.pirandola@york.ac.uk).

Quantum information[1–3] is evolving towards next-generation quantum technologies, such as the realization of completely secure quantum communications[4–6] and the long-term construction of a quantum Internet[7–10]. But quantum information is more fragile than its classical counterpart, so that the ideal performances of quantum protocols may rapidly degrade in realistic practical implementations. In particular, this is a basic limitation that affects any point-to-point protocol of quantum communication over a quantum channel, where two remote parties transmit qubits, distribute entanglement or secret keys. In this communication context, it is a crucial open problem to determine the ultimate rates achievable by the remote parties, assuming that they may apply arbitrary local operations (LOs) assisted by unlimited two-way classical communication (CCs), that we may briefly call adaptive LOCCs. The maximum rates achievable by these adaptive protocols are known as two-way (assisted) capacities of a quantum channel and represent fundamental benchmarks for quantum repeaters[11].

Before our work, a single two-way capacity was known, discovered about 20 years ago[12]. For the important case of bosonic channels[2], there were only partial results. Building on previous ideas[13], ref. 14 introduced the reverse coherent information. By exploiting this notion and other tools[15,16], the authors of ref. 17 established lower bounds for the two-way capacities of a Gaussian channel. This inspired a subsequent work[18], which exploited the notion of squashed entanglement[19] to build upper bounds; unfortunately the latter were too large to close the gap with the best-known lower bounds.

Our work addresses this basic problem. We devise a general methodology that completely simplifies the study of adaptive protocols and allows us to upperbound the two-way capacities of an arbitrary quantum channel with a computable single-letter quantity. In this way, we are able to establish exact formulas for the two-way capacities of several fundamental channels, such as bosonic lossy channels, quantum-limited amplifiers, dephasing and erasure channels in arbitrary dimension. For these channels, we determine the ultimate rates for transmitting quantum information (two-way quantum capacity Q_2), distributing entanglement (two-way entanglement distribution capacity D_2) and generating secret keys (secret-key capacity K). In particular, we establish the exact rate-loss scaling that restricts any point-to-point protocol of quantum key distribution (QKD) when implemented through a lossy communication line, such as an optical fibre or a free-space link.

Results

General overview of the results. As already mentioned in the Introduction, we establish the two-way capacities (Q_2, D_2 and K) for a number of quantum channels at both finite and infinite dimension, that is, we consider channels defined on both discrete variable (DV) and continuous variable (CV) systems[2]. Two-way capacities are benchmarks for quantum repeaters because they are derived by removing any technical limitation from the point-to-point protocols between the remote parties, who may perform the most general strategies allowed by quantum mechanics in the absence of pre-shared entanglement. Clearly, these ultimate limits cannot be achieved by imposing restrictions on the number of channel uses or enforcing energy constraints at the input. The relaxation of such constraints has also practical reasons since it approximates the working regime of current QKD protocols, that exploit large data blocks and high-energy Gaussian modulations[13,20].

To achieve our results we suitably combine the relative entropy of entanglement (REE)[21–23] with teleportation[9,24–26] to design a general reduction method, which remarkably simplifies the study of adaptive protocols and two-way capacities. The first step is to show that the two-way capacities of a quantum channel cannot exceed a general bound based on the REE. The second step is the application of a technique, dubbed ‘teleportation stretching’, which is valid for any channel at any dimension. This allows us to reduce any adaptive protocol into a block form, so that the general REE bound becomes a single-letter quantity. In this way, we easily upperbound the two-way capacities of any quantum channel, with closed formulas proven for bosonic Gaussian channels[2], Pauli channels, erasure channels and amplitude damping channels[1].

Most importantly, by showing coincidence with suitable lower bounds, we prove simple formulas for the two-way quantum capacity Q_2 $(=D_2)$ and the secret-key capacity K of several fundamental channels. In fact, for the erasure channel we show that $K=1-p$ where p is the erasure probability (only its Q_2 was previously known[12]); for the dephasing channel we show that $Q_2=K=1-H_2(p)$, where H_2 is the binary Shannon entropy and p is the dephasing probability (these results for qubits are extended to any finite dimension). Then, for a quantum-limited amplifier, we show that $Q_2=K=-\log_2(1-g^{-1})$ where g is the gain. Finally, for the lossy channel, we prove that $Q_2=K=-\log_2(1-\eta)$ where η is the transmissivity. In particular, the secret-key capacity of the lossy channel is the maximum rate achievable by any optical implementation of QKD. At long distance, that is, high loss $\eta\simeq 0$, we find the optimal rate-loss scaling of $K\simeq 1.44\,\eta$ secret bits per channel use, a fundamental bound that only quantum repeaters may surpass.

In the following, we start by giving the main definitions. Then we formulate our reduction method and we derive the analytical results for the various quantum channels.

Adaptive protocols and two-way capacities. Suppose that Alice and Bob are separated by a quantum channel $\mathcal{E}$ and want to implement the most general protocol assisted by adaptive LOCCs. This protocol may be stated for an arbitrary quantum task and then specified for the transmission of quantum information, distribution of entanglement or secret correlations. Assume that Alice and Bob have countable sets of systems, $\mathbf{a}$ and $\mathbf{b}$, respectively. These are local registers which are updated before and after each transmission. The steps of an arbitrary adaptive protocol are described in Fig. 1.

After n transmissions, Alice and Bob share an output state $\rho^n_{\mathbf{ab}}:=\rho_{\mathbf{ab}}(\mathcal{E}^{\otimes n})$ depending on the sequence of adaptive LOCCs

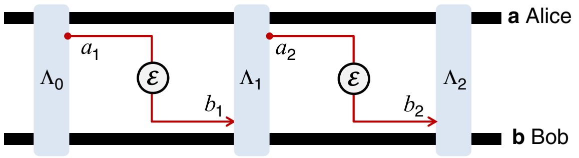

Figure 1 | Adaptive quantum protocol. The first step is the preparation of the initial separable state $\rho^0_{\mathbf{ab}}$ of $\mathbf{a}$ and $\mathbf{b}$ by some adaptive LOCC Λ_0. After the preparation of the local registers, there is the first transmission: Alice picks a system from her local register $a_1\in\mathbf{a}$, so that the register is updated as $\mathbf{a}\rightarrow\mathbf{a}a_1$; system a_1 is sent through the channel $\mathcal{E}$, with Bob getting the output b_1; Bob includes the output in his local register, which is updated as $b_1\mathbf{b}\rightarrow\mathbf{b}$; finally, Alice and Bob apply another adaptive LOCC Λ_1 to their registers $\mathbf{a}$,$\mathbf{b}$. In the second transmission, Alice picks and sends another system $a_2\in\mathbf{a}$ through channel $\mathcal{E}$ with output b_2 for Bob. The parties apply a further adaptive LOCC Λ_2 to their registers and so on. This procedure is repeated n times, with output state $\rho^n_{\mathbf{ab}}$ for the Alice's and Bob's local registers.

$\mathcal{L}=\{\Lambda_0,\cdots,\Lambda_n\}$. By definition, this adaptive protocol has a rate equal to R_n if the output $\rho^n_{\mathbf{ab}}$ is sufficiently close to a target state ϕ_n with nR_n bits, that is, we may write $\left\|\rho^n_{\mathbf{ab}}-\phi_n\right\|\leq\varepsilon$ in trace norm. The rate of the protocol is an average quantity, which means that the sequence $\mathcal{L}$ is assumed to be averaged over local measurements, so that it becomes trace-preserving. Thus, by taking the asymptotic limit in n and optimizing over $\mathcal{L}$, we define the generic two-way capacity of the channel as

$$\mathcal{C}(\mathcal{E}):=\sup_{\mathcal{L}}\lim_{n}R_n. \tag{1}$$

In particular, if the aim of the protocol is entanglement distribution, then the target state ϕ_n is a maximally entangled state and $\mathcal{C}(\mathcal{E})=D_2(\mathcal{E})$. Because an ebit can teleport a qubit and a qubit can distribute an ebit, $D_2(\mathcal{E})$ coincides with the two-way quantum capacity $Q_2(\mathcal{E})$. If the goal is to implement QKD, then the target state ϕ_n is a private state[27] and $\mathcal{C}(\mathcal{E})=K(\mathcal{E})$. Here the secret-key capacity satisfies $K(\mathcal{E})\geq D_2(\mathcal{E})$, because ebits are specific types of secret bits and LOCCs are equivalent to LOs and public communication[27]. Thus, the generic two-way capacity $\mathcal{C}$ can be any of D_2, Q_2 or K, and these capacities must satisfy $D_2=Q_2\leq K$. Also, note that we may consider the two-way private capacity $P_2(\mathcal{E})$, which is the maximum rate at which classical messages can be securely transmitted[15]. Because of the unlimited two-way CCs and the one-time pad, we have $P_2(\mathcal{E})=K(\mathcal{E})$, so that this equivalence is implicitly assumed hereafter.

General bounds for two-way capacities. Let us design suitable bounds for $\mathcal{C}(\mathcal{E})$. From below we know that we may use the coherent[28,29] or reverse coherent[14,17] information. Take a maximally entangled state of two systems A and B, that is, an Einstein–Podolsky–Rosen (EPR) state Φ_{AB}. Propagating the B-part through the channel defines its Choi matrix $\rho_{\mathcal{E}}:=\mathcal{I}\otimes\mathcal{E}(\Phi_{AB})$. This allows us to introduce the coherent information of the channel $I_{\mathrm{C}}(\mathcal{E})$ and its reverse counterpart $I_{\mathrm{RC}}(\mathcal{E})$, defined as $I_{\mathrm{C(RC)}}(\mathcal{E}):=S\left[\mathrm{Tr}_{A(B)}(\rho_{\mathcal{E}})\right]-S(\rho_{\mathcal{E}})$, where $S(\cdot)$ is the von Neumann entropy. These quantities represent lower bounds for the entanglement that is distillable from the Choi matrix $\rho_{\mathcal{E}}$ via one-way CCs, denoted as $D_1(\rho_{\mathcal{E}})$. In other words, we can write the hashing inequality[16]

$$\max\{I_{\mathrm{C}}(\mathcal{E}),I_{\mathrm{RC}}(\mathcal{E})\}\leq D_1(\rho_{\mathcal{E}})\leq\mathcal{C}(\mathcal{E}). \tag{2}$$

For bosonic systems, the ideal EPR state has infinite-energy, so that the Choi matrix of a bosonic channel is energy-unbounded (see Methods for notions on bosonic systems). In this case we consider a sequence of two-mode squeezed vacuum (TMSV) states[2] Φ^μ with variance $\mu=\bar{n}+1/2$, where $\bar{n}$ is the mean number of thermal photons in each mode. This sequence defines the bosonic EPR state as $\Phi:=\lim_\mu\Phi^\mu$. At the output of the channel, we have the sequence of quasi-Choi matrices

$$\rho^\mu_{\mathcal{E}}:=\mathcal{I}\otimes\mathcal{E}(\Phi^\mu), \tag{3}$$

defining the asymptotic Choi matrix $\rho_{\mathcal{E}}:=\lim_\mu\rho^\mu_{\mathcal{E}}$. As a result, the coherent information quantities must be computed as limits on $\rho^\mu_{\mathcal{E}}$ and the hashing inequality needs to be suitably extended (see Supplementary Note 2, which exploits the truncation tools of Supplementary Note 1).

In this work the crucial tool is the upper bound. Recall that, for any bipartite state ρ, the REE is defined as $E_{\mathrm{R}}(\rho)=\inf_{\sigma_s}S(\rho\|\sigma_s)$, where σ_s is an arbitrary separable state and $S(\rho\|\sigma_s):=\mathrm{Tr}\left[\rho\left(\log_2\rho-\log_2\sigma_s\right)\right]$ is the relative entropy[23]. Hereafter we extend this definition to include asymptotic (energy-unbounded) states. For an asymptotic state $\sigma:=\lim_\mu\sigma^\mu$ defined by a sequence of states σ^μ, we define its REE as

$$E_{\mathrm{R}}(\sigma):=\inf_{\sigma^\mu_s}\liminf_{\mu\to+\infty}S\left(\sigma^\mu\|\sigma^\mu_s\right), \tag{4}$$

where σ^μ_s is an arbitrary sequence of separable states such that $\left\|\sigma^\mu_s-\sigma_s\right\|\to0$ for some separable σ_s. In general, we also consider the regularized REE

$$E^\infty_{\mathrm{R}}(\sigma):=\lim_n n^{-1}E_{\mathrm{R}}(\sigma^{\otimes n})\leq E_{\mathrm{R}}(\sigma), \tag{5}$$

where $\sigma^{\otimes n}:=\lim_\mu\sigma^{\mu\otimes n}$ for an asymptotic state σ.

Thus, the REE of a Choi matrix $E_{\mathrm{R}}(\rho_{\mathcal{E}})$ is correctly defined for channels of any dimension, both finite and infinite. We may also define the channel's REE as

$$E_{\mathrm{R}}(\mathcal{E}):=\sup_\rho E_{\mathrm{R}}[\mathcal{I}\otimes\mathcal{E}(\rho)]\geq E_{\mathrm{R}}(\rho_{\mathcal{E}}), \tag{6}$$

where the supremum includes asymptotic states for bosonic channels. In the following, we prove that these single-letter quantities, $E_{\mathrm{R}}(\mathcal{E})$ and $E_{\mathrm{R}}(\rho_{\mathcal{E}})$, bound the two-way capacity $\mathcal{C}(\mathcal{E})$ of basic channels. The first step is the following general result.

Theorem 1 (*general weak converse*): At any dimension, finite or infinite, the generic two-way capacity of a quantum channel $\mathcal{E}$ is upper bounded by the REE bound

$$\mathcal{C}(\mathcal{E})\leq E^\star_{\mathrm{R}}(\mathcal{E}):=\sup_{\mathcal{L}}\lim_n\frac{E_{\mathrm{R}}\left(\rho^n_{\mathbf{ab}}\right)}{n}. \tag{7}$$

In Supplementary Note 3, we provide various equivalent proofs. The simplest one assumes an exponential growth of the shield system in the target private state[27] as proven by ref. 30 and trivially adapted to CVs. Another proof is completely independent from the shield system. Once established the bound $E^\star_{\mathrm{R}}(\mathcal{E})$, our next step is to simplify it by applying the technique of teleportation stretching, which is in turn based on a suitable simulation of quantum channels.

Simulation of quantum channels. The idea of simulating channels by teleportation was first developed[31,32] for Pauli channels[33], and further studied in finite dimension[34–36] after the introduction of generalized teleportation protocols[37]. Then, ref. 38 moved the first steps in the simulation of Gaussian channels via the CV teleportation protocol[25,26]. Another type of simulation is a deterministic version[39] of a programmable quantum gate array[40]. Developed for DV systems, this is based on joint quantum operations, therefore failing to catch the LOCC structure of quantum communication. Here not only we fully extend the teleportation-simulation to CV systems, but we also design the most general channel simulation in a communication scenario; this is based on arbitrary LOCCs and may involve systems of any dimension, finite or infinite (see Supplementary Note 8 for comparisons and advances).

As explained in Fig. 2a, performing a teleportation LOCC (that is, Bell detection and unitary corrections) over a mixed state σ is a way to simulate a (certain type of) quantum channel $\mathcal{E}$ from Alice to Bob. However, more generally, the channel simulation can be realized using an arbitrary trace-preserving LOCC $\mathcal{T}$ and an arbitrary resource state σ (see Fig. 2b). Thus, at any dimension, we say that a channel $\mathcal{E}$ is 'σ-stretchable' or 'stretchable into σ' if there is a trace-preserving LOCC $\mathcal{T}$ such that

$$\mathcal{E}(\rho)=\mathcal{T}(\rho\otimes\sigma). \tag{8}$$

In general, we can simulate the same channel $\mathcal{E}$ with different choices of $\mathcal{T}$ and σ. In fact, any channel is stretchable into some state σ: A trivial choice is decomposing $\mathcal{E}=\mathcal{I}\circ\mathcal{E}$, inserting $\mathcal{E}$ in Alice's LO and simulating $\mathcal{I}$ with teleportation over the ideal EPR state $\sigma=\Phi$. Therefore, among all simulations, one needs to identify the best resource state that optimizes the functional under study. In our work, the best results are achieved when the state σ can be chosen as the Choi matrix of the channel. This is not a property of any channel but defines a class. Thus, we define 'Choi-stretchable' a channel that can be LOCC-simulated over its

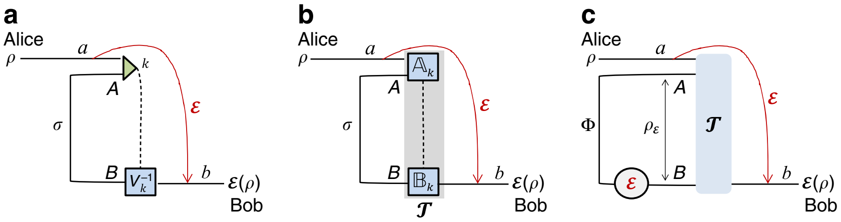

Figure 2 | From teleportation- to LOCC-simulation of quantum channels. (**a**) Consider the generalized teleportation of an input state ρ of a d-dimensional system a by using a resource state σ of two systems, A and B, with corresponding dimensions d and d' (finite or infinite). Systems a and A are subject to a Bell detection (triangle) with random outcome k. This outcome is associated with a projection onto a maximally entangled state up to an associated teleportation unitary U_k which is a Pauli operator for $d < +\infty$ and a phase-displacement for $d = +\infty$ (see Methods for the basics of quantum teleportation and the characterization of the teleportation unitaries). The classical outcome k is communicated to Bob, who applies a correction unitary V_k^{-1} to his system B with output b. In general, V_k does not necessarily belong to the set $\{U_k\}$. On average, this teleportation LOCC defines a teleportation channel $\mathcal{E}$ from a to b. It is clear that this construction also teleports part a of an input state involving ancillary systems. (**b**) In general we may replace the teleportation LOCC (Bell detection and unitary corrections) with an arbitrary LOCC $\mathcal{T}$: Alice performs a quantum operation $\mathbb{A}_k$ on her systems a and A, communicates the classical variable k to Bob, who then applies another quantum operation $\mathbb{B}_k$ on his system B. By averaging over the variable k, so that $\mathcal{T}$ is certainly trace-preserving, we achieve the simulation $\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \sigma)$ for any input state ρ. We say that a channel $\mathcal{E}$ is 'σ-stretchable' if it can be simulated by a resource state σ for some LOCC $\mathcal{T}$. Note that Alice's and Bob's LOs $\mathbb{A}_k$ and $\mathbb{B}_k$ are arbitrary quantum operations; they may involve other local ancillas and also have extra labels (due to additional local measurements), in which case $\mathcal{T}$ is assumed to be averaged over all these labels. (**c**) The most important case is when channel $\mathcal{E}$ can be simulated by a trace-preserving LOCC $\mathcal{T}$ applied to its Choi matrix $\rho_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi)$, with Φ being an EPR state. In this case, we say that the channel is 'Choi-stretchable'. These definitions are suitably extended to bosonic channels.

Choi matrix, so that we may write equation (8) with $\sigma = \rho_{\mathcal{E}}$ (see also Fig. 2c).

In infinite dimension, the LOCC simulation may involve limits $\mathcal{T} := \lim_\mu \mathcal{T}^\mu$ and $\sigma := \lim_\mu \sigma^\mu$ of sequences $\mathcal{T}^\mu$ and σ^μ. For any finite μ, the simulation $(\mathcal{T}^\mu, \sigma^\mu)$ provides some teleportation channel $\mathcal{E}^\mu$. Now, suppose that an asymptotic channel $\mathcal{E}$ is defined as a pointwise limit of the sequence $\mathcal{E}^\mu$, that is, we have $\|\mathcal{I} \otimes \mathcal{E}(\rho) - \mathcal{I} \otimes \mathcal{E}^\mu(\rho)\| \xrightarrow{\mu} 0$ for any bipartite state ρ. Then, we say that $\mathcal{E}$ is stretchable with asymptotic simulation $(\mathcal{T}, \sigma)$. This is important for bosonic channels, for which Choi-based simulations can only be asymptotic and based on sequences $\rho_{\mathcal{E}}^\mu$.

Teleportation covariance. We now discuss a property which easily identifies Choi-stretchable channels. Call $\mathbb{U}_d$ the random unitaries which are generated by the Bell detection in a teleportation process. For a qudit, $\mathbb{U}_d$ is composed of generalized Pauli operators, that is, the generators of the Weyl–Heisenberg group. For a CV system, the set $\mathbb{U}_\infty$ is composed of displacement operators[9], spanning the infinite dimensional version of the previous group. In arbitrary dimension (finite or infinite), we say that a quantum channel is 'teleportation-covariant' if, for any teleportation unitary $U \in \mathbb{U}_d$, we may write

$$\mathcal{E}\left(U \rho U^\dagger\right) = V \mathcal{E}(\rho) V^\dagger, \qquad (9)$$

for some another unitary V (not necessarily in $\mathbb{U}_d$).

The key property of a teleportation-covariant channel is that the input teleportation unitaries can be pushed out of the channel, where they become other correctable unitaries. Because of this property, the transmission of a system through the channel can be simulated by a generalized teleportation protocol over its Choi matrix. This is the content of the following proposition.

Proposition 2 (*tele-covariance*): At any dimension, a teleportation-covariant channel $\mathcal{E}$ is Choi-stretchable. The simulation is a teleportation LOCC over its Choi matrix $\rho_{\mathcal{E}}$, which is asymptotic for a bosonic channel.

The simple proof is explained in Fig. 3. The class of teleportation-covariant channels is wide and includes bosonic Gaussian channels, Pauli and erasure channels at any dimension (see Methods for a more detailed classification). All these fundamental channels are therefore Choi-stretchable. There are channels that are not (or not known to be) Choi-stretchable but still have decompositions $\mathcal{E} = \mathcal{E}'' \circ \tilde{\mathcal{E}} \circ \mathcal{E}'$ where the middle part $\tilde{\mathcal{E}}$ is Choi-stretchable. In this case, $\mathcal{E}'$ and $\mathcal{E}''$ can be made part of Alice's and Bob's LOs, so that channel $\mathcal{E}$ can be stretched into the state $\sigma = \rho_{\tilde{\mathcal{E}}}$. An example is the amplitude damping channel as we will see afterwards.

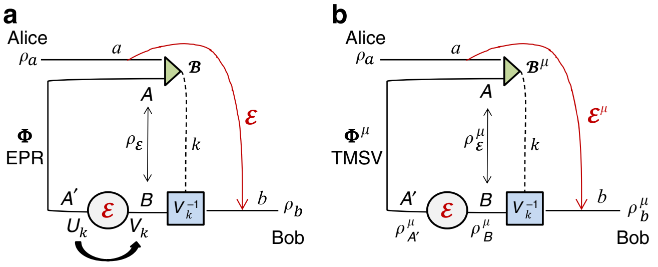

Figure 3 | Teleportation-covariant channels are Choi-stretchable. (**a**) Consider the teleportation of an input state ρ_a by using an EPR state $\Phi_{AA'}$ of systems A and A'. The Bell detection $\mathcal{B}$ on systems a and A teleports the input state onto A', up to a random teleportation unitary, that is, $\rho_{A'} = U_k \rho_a U_k^\dagger$. Because $\mathcal{E}$ is teleportation-covariant, U_k is mapped into an output unitary V_k and we may write $\rho_B = \mathcal{E}(\rho_{A'}) = \mathcal{E}\left(U_k \rho_a U_k^\dagger\right) = V_k \mathcal{E}(\rho_a) V_k^\dagger$. Therefore, Bob just needs to receive the outcome k and apply V_k^{-1}, so that $\rho_b = V_k^{-1} \rho_B \left(V_k^{-1}\right)^\dagger = \mathcal{E}(\rho_a)$. Globally, the process describes the simulation of channel $\mathcal{E}$ by means of a generalized teleportation protocol over the Choi matrix $\rho_{\mathcal{E}}$. (**b**) The procedure is also valid for CV systems. If the input a is a bosonic mode, we need to consider finite-energy versions for the EPR state Φ and the Bell detection $\mathcal{B}$, that is, we use a TMSV state Φ^μ and a corresponding quasi-projection $\mathcal{B}^\mu$ onto displaced TMSV states. At finite energy μ, the teleportation process from a to A' is imperfect with some output $\rho_{A'}^\mu \neq \rho_{A'} = U_k \rho_a U_k^\dagger$. However, for any $\varepsilon > 0$ and input state ρ_a, there is a sufficiently large value of μ such that $\left\|\rho_{A'}^\mu - \rho_{A'}\right\| \leq \varepsilon$ (refs 25,26). Consider the transmitted state $\rho_B^\mu = \mathcal{E}\left(\rho_{A'}^\mu\right)$. Because the trace distance decreases under channels, we have $\left\|\rho_B^\mu - \rho_B\right\| \leq \left\|\rho_{A'}^\mu - \rho_{A'}\right\| \leq \varepsilon$. After the application of the correction unitary V_k^{-1}, we have the output state ρ_b^μ which satisfies $\left\|\rho_b^\mu - \mathcal{E}(\rho_a)\right\| \leq \varepsilon$. Taking the asymptotic limit of large μ, we achieve $\left\|\rho_b^\mu - \mathcal{E}(\rho_a)\right\| \to 0$ for any input ρ_a, therefore achieving the perfect asymptotic simulation of the channel. The asymptotic teleportation-LOCC is therefore $(\mathcal{B}, \rho_{\mathcal{E}}) := \lim_\mu \left(\mathcal{B}^\mu, \rho_{\mathcal{E}}^\mu\right)$ where $\rho_{\mathcal{E}}^\mu := \mathcal{I} \otimes \mathcal{E}(\Phi^\mu)$. The result is trivially extended to the presence of ancillas.

Teleportation stretching of adaptive protocols. We are now ready to describe the reduction of arbitrary adaptive protocols. The procedure is schematically shown in Fig. 4. We start by considering the ith transmission through the channel $\mathcal{E}$, so that Alice and Bob's register state is updated from $\rho^{i-1}_{\mathbf{ab}}$ to $\rho^{i}_{\mathbf{ab}}$. By using a simulation $(\mathcal{T},\sigma)$, we show the input–output formula

$$\rho^{i}_{\mathbf{ab}} = \Delta_i\left(\rho^{i-1}_{\mathbf{ab}} \otimes \sigma\right), \tag{10}$$

for some 'extended' LOCC Δ_i (Fig. 4c). By iterating the previous formula n times, we may write the output state $\rho^{n}_{\mathbf{ab}} = \Lambda(\rho^{0}_{\mathbf{ab}} \otimes \sigma^{\otimes n})$ for $\Lambda := \Delta_n \circ \ldots \circ \Delta_1$ (as in Fig. 4d). Because the initial state $\rho^{0}_{\mathbf{ab}}$ is separable, its preparation can be included in Λ and we may directly write $\rho^{n}_{\mathbf{ab}} = \Lambda(\sigma^{\otimes n})$. Finally, we average over all local measurements present in Λ, so that $\rho^{n}_{\mathbf{ab}} = \bar{\Lambda}(\sigma^{\otimes n})$ for a trace-preserving LOCC $\bar{\Lambda}$ (Fig. 4e). More precisely, for any sequence of outcomes $\mathbf{u}$ with probability $p(\mathbf{u})$, there is a conditional LOCC $\Lambda_{\mathbf{u}}$ with output $\rho^{n}_{\mathbf{ab}}(\mathbf{u}) = p(\mathbf{u})^{-1}\Lambda_{\mathbf{u}}(\sigma^{\otimes n})$. Thus, the mean output state $\rho^{n}_{\mathbf{ab}}$ is generated by $\bar{\Lambda} = \sum_{\mathbf{u}}\Lambda_{\mathbf{u}}$ (see Methods for more technical details on this LOCC averaging).

Note that the simulation of a bosonic channel $\mathcal{E}$ is typically asymptotic, with infinite-energy limits $\mathcal{T} := \lim_\mu \mathcal{T}^\mu$ and $\sigma := \lim_\mu \sigma^\mu$. In this case, we repeat the procedure for some μ, with output $\rho^{n,\mu}_{\mathbf{ab}} := \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})$, where $\bar{\Lambda}_\mu$ is derived assuming the finite-energy LOCCs $\mathcal{T}^\mu$. Then, we take the limit for large μ, so that $\rho^{n,\mu}_{\mathbf{ab}}$ converges to $\rho^{n}_{\mathbf{ab}}$ in trace norm (see Methods for details on teleportation stretching with bosonic channels). Thus, at any dimension, we have proven the following result.

Lemma 3 *(Stretching)*: Consider arbitrary n transmissions through a channel $\mathcal{E}$ which is stretchable into a resource state σ. The output of an adaptive protocol can be decomposed into the block form

$$\rho^{n}_{\mathbf{ab}} = \bar{\Lambda}(\sigma^{\otimes n}), \tag{11}$$

for some trace-preserving LOCC $\bar{\Lambda}$. If the channel $\mathcal{E}$ is Choi-stretchable, then we may write

$$\rho^{n}_{\mathbf{ab}} = \bar{\Lambda}\left(\rho_{\mathcal{E}}^{\otimes n}\right). \tag{12}$$

In particular, $\bar{\Lambda}(\sigma^{\otimes n}) := \lim_\mu \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})$ for an asymptotic channel simulation $(\mathcal{T},\sigma) := \lim_\mu(\mathcal{T}^\mu, \sigma^\mu)$.

According to this Lemma, teleportation stretching reduces an adaptive protocol performing an arbitrary task (quantum communication, entanglement distribution or key generation) into an equivalent block protocol, whose output state $\rho^{n}_{\mathbf{ab}}$ is the same but suitably decomposed as in equation (11) for any number n of channel uses. In particular, for Choi-stretchable channels, the output is decomposed into a tensor product of Choi matrices. An essential feature that makes the technique applicable to many contexts is the fact that the adaptive-to-block reduction maintains task and output of the original protocol so that, for example, adaptive key generation is reduced to block key generation and not entanglement distillation.

Remark 4: Some aspects of our method might be traced back to a precursory but very specific argument discussed in Section V of ref. 31, where protocols of quantum communication (through Pauli channels) were transformed into protocols of entanglement distillation (the idea was developed for one-way CCs, with an implicit extension to two-way CCs). However, while this argument may be seen as precursory, it is certainly not developed at the level of generality of the present work where the adaptive-to-block reduction is explicitly proven for any type of protocol and any channel at any dimension (see Supplementary Notes 9 and 10 for remarks on previous literature).

REE as a single-letter converse bound. The combination of Theorem 1 and Lemma 3 provides the insight of our entire reduction method. In fact, let us compute the REE of the output state $\rho^{n}_{\mathbf{ab}}$, decomposed as in equation (11). Using the monotonicity of the REE under trace-preserving LOCCs, we derive

$$E_{\mathrm{R}}\left(\rho^{n}_{\mathbf{ab}}\right) \leq E_{\mathrm{R}}(\sigma^{\otimes n}), \tag{13}$$

where the complicated $\bar{\Lambda}$ is fully discarded. Then, by replacing equation (13) into equation (7), we can ignore the supremum in the definition of $E^{\star}_{\mathrm{R}}(\mathcal{E})$ and get the simple bound

$$E^{\star}_{\mathrm{R}}(\mathcal{E}) \leq E^{\infty}_{\mathrm{R}}(\sigma) \leq E_{\mathrm{R}}(\sigma). \tag{14}$$

Thus, we can state the following main result.

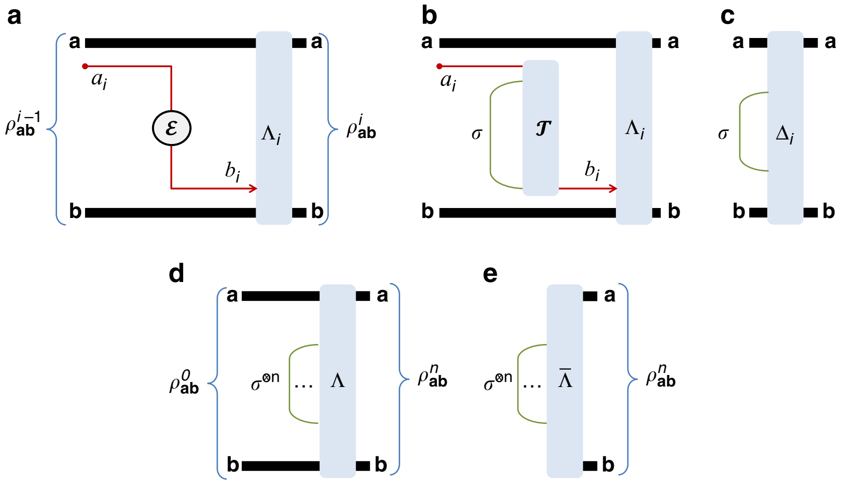

Figure 4 | Teleportation stretching of an adaptive quantum protocol. (**a**) Consider the ith transmission through channel $\mathcal{E}$, where the input $(i-1)$th register state is given by $\rho^{i-1}_{\mathbf{ab}} := \rho_{\mathbf{a}a_i\mathbf{b}}$. After transmission through $\mathcal{E}$ and the adaptive LOCC Λ_i, the register state is updated to $\rho^{i}_{\mathbf{ab}} = \Lambda_i \circ (\mathcal{I}_{\mathbf{a}} \otimes \mathcal{E} \otimes \mathcal{I}_{\mathbf{b}})(\rho_{\mathbf{a}a_i\mathbf{b}})$. (**b**) Let us simulate the channel $\mathcal{E}$ by a LOCC $\mathcal{T}$ and a resource state σ. (**c**) The simulation LOCC $\mathcal{T}$ can be combined with the adaptive LOCC Λ_i into a single 'extended' LOCC Δ_i while the resource state σ can be stretched back in time and out of the adaptive operations. We may therefore write $\rho^{i}_{\mathbf{ab}} = \Delta_i(\rho^{i-1}_{\mathbf{ab}} \otimes \sigma)$. (**d**) We iterate the previous steps for all transmissions, so as to stretch n copies $\sigma^{\otimes n}$ and collapse all the extended LOCCs Δ_n o …o Δ_1 into a single LOCC Λ. In other words, we may write $\rho^{n}_{\mathbf{ab}} = \Lambda(\rho^{0}_{\mathbf{ab}} \otimes \sigma^{\otimes n})$. (**e**) Finally, we include the preparation of the separable state $\rho^{0}_{\mathbf{ab}}$ into Λ and we also average over all local measurements present in Λ, so that we may write the output state as $\rho^{n}_{\mathbf{ab}} = \bar{\Lambda}(\sigma^{\otimes n})$ for a trace-preserving LOCC $\bar{\Lambda}$. The procedure is asymptotic in the presence of asymptotic channel simulations (bosonic channels).

Theorem 5 (*one-shot REE bound*): Let us stretch an arbitrary quantum channel $\mathcal{E}$ into some resource state σ, according to equation (8). Then, we may write

$$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}^{\infty}(\sigma) \leq E_{\mathrm{R}}(\sigma). \quad (15)$$

In particular, if $\mathcal{E}$ is Choi-stretchable, we have

$$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}}) \leq E_{\mathrm{R}}(\rho_{\mathcal{E}}) = E_{\mathrm{R}}(\mathcal{E}). \quad (16)$$

See Methods for a detailed proof, with explicit derivations for bosonic channels. We have therefore reached our goal and found single-letter bounds. In particular, note that $E_{\mathrm{R}}(\rho_{\mathcal{E}})$ measures the entanglement distributed by a single EPR state, so that we may call it the 'entanglement flux' of the channel $\Phi(\mathcal{E}):=E_{\mathrm{R}}(\rho_{\mathcal{E}})$. Remarkably, there is a sub-class of Choi-stretchable channels for which $E_{\mathrm{R}}(\rho_{\mathcal{E}})$ coincides with the lower bound $D_1(\rho_{\mathcal{E}})$ in equation (2). We call these 'distillable channels'. We establish all their two-way capacities as $\mathcal{C}(\mathcal{E})=E_{\mathrm{R}}(\rho_{\mathcal{E}})$. They include lossy channels, quantum-limited amplifiers, dephasing and erasure channels. See also Fig. 5.

Immediate generalizations. Consider a fading channel, described by an ensemble $\{p_i, \mathcal{E}_i\}$, where channel $\mathcal{E}_i$ occurs with probability p_i. Let us stretch $\mathcal{E}_i$ into a resource state σ_i. For large n, we may decompose the output of an adaptive protocol as $\rho_{\mathbf{ab}}^n = \bar{\Lambda}\left(\otimes_i \sigma_i^{\otimes np_i}\right)$, so that the two-way capacity of this channel is bounded by

$$\mathcal{C}(\{p_i, \mathcal{E}_i\}) \leq \sum_i p_i E_{\mathrm{R}}(\sigma_i). \quad (17)$$

Then consider adaptive protocols of two-way quantum communication, where the parties have forward ($\mathcal{E}$) and backward ($\mathcal{E}'$) channels. The capacity $\mathcal{C}(\mathcal{E},\mathcal{E}')$ maximizes the number of target bits per channel use. Stretching $(\mathcal{E},\mathcal{E}')$ into a pair of states (σ, σ'), we find $\mathcal{C}(\mathcal{E},\mathcal{E}') \leq \max\{E_{\mathrm{R}}(\sigma), E_{\mathrm{R}}(\sigma')\}$. For Choi-stretchable channels, this means $\mathcal{C}(\mathcal{E},\mathcal{E}') \leq \max\{\Phi(\mathcal{E}), \Phi(\mathcal{E}')\}$, which reduces to $\mathcal{C}(\mathcal{E},\mathcal{E}')=\max\{\mathcal{C}(\mathcal{E}),\mathcal{C}(\mathcal{E}')\}$ if they are distillable. In the latter case, the optimal strategy is using the channel with the maximum capacity (see Methods).

Yet another scenario is the multiband channel $\mathcal{E}_{\mathrm{mb}}$, where Alice exploits m independent channels or 'bands' $\{\mathcal{E}_i\}$, so that the capacity $\mathcal{C}(\mathcal{E}_{\mathrm{mb}})$ maximizes the number of target bits per multiband transmission. By stretching the bands $\{\mathcal{E}_i\}$ into resource states $\{\sigma_i\}$, we find $\mathcal{C}(\mathcal{E}_{\mathrm{mb}}) \leq \sum_i E_{\mathrm{R}}(\sigma_i)$. For Choi-stretchable bands, this means $\mathcal{C}(\mathcal{E}_{\mathrm{mb}}) \leq \sum_i \Phi(\mathcal{E}_i)$, giving the additive capacity $\mathcal{C}(\mathcal{E}_{\mathrm{mb}}) = \sum_i \mathcal{C}(\mathcal{E}_i)$ if they are distillable (see Methods).

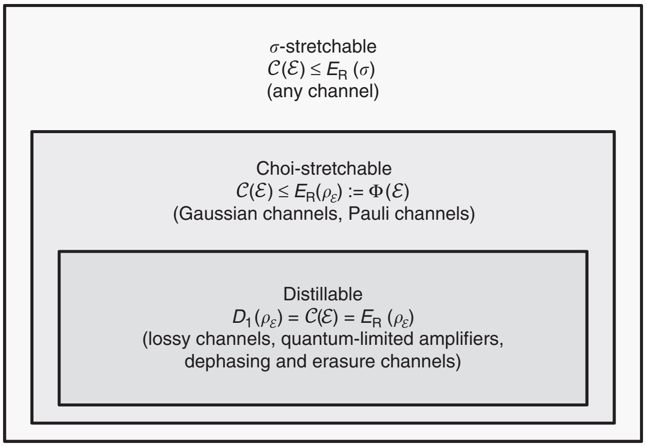
σ-stretchable
$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}(\sigma)$
(any channel)
Choi-stretchable
$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}(\rho_{\mathcal{E}}) := \Phi(\mathcal{E})$
(Gaussian channels, Pauli channels)
Distillable
$D_1(\rho_{\mathcal{E}}) = \mathcal{C}(\mathcal{E}) = E_{\mathrm{R}}(\rho_{\mathcal{E}})$
(lossy channels, quantum-limited amplifiers,
dephasing and erasure channels)

Figure 5 | Classification of channels in DVs and CVs. We depict the classes of channels that are considered in this work, together with the bounds for their two-way capacities.

Ultimate limits of bosonic communications. We now apply our method to derive the ultimate rates for quantum and secure communication through bosonic Gaussian channels. These channels are Choi-stretchable with an asymptotic simulation involving $\rho_{\mathcal{E}} := \lim_{\mu} \rho_{\mathcal{E}}^{\mu}$. From equations (4) and (16), we may write

$$\mathcal{C}(\mathcal{E}) \leq \Phi(\mathcal{E}) \leq \liminf_{\mu \to +\infty} S\left(\rho_{\mathcal{E}}^{\mu} \middle\| \tilde{\sigma}_s^{\mu}\right), \quad (18)$$

for a suitable converging sequence of separable states $\tilde{\sigma}_s^{\mu}$.

For Gaussian channels, the sequences in equation (18) involve Gaussian states, for which we easily compute the relative entropy. In fact, for any two Gaussian states, ρ_1 and ρ_2, we prove the general formula $S(\rho_1\|\rho_2)=\Sigma(V_1, V_2)-S(\rho_1)$, where Σ is a simple functional of their statistical moments (see Methods). After technical derivations (Supplementary Note 4), we then bound the two-way capacities of all Gaussian channels, starting from the most important, the lossy channel.

Fundamental rate-loss scaling. Optical communications through free-space links or telecom fibres are inevitably lossy and the standard model to describe this scenario is the lossy channel. This is a bosonic Gaussian channel characterized by a transmissivity parameter η, which quantifies the fraction of input photons surviving the channel. It can be represented as a beam splitter mixing the signals with a zero-temperature environment (background thermal noise is negligible at optical and telecom frequencies).

For a lossy channel $\mathcal{E}_\eta$ with arbitrary transmissivity η we apply our reduction method and compute the entanglement flux $\Phi(\eta) \leq -\log_2(1-\eta)$. This coincides with the reverse coherent information of this channel $I_{\mathrm{RC}}(\eta)$, first derived in ref. 17. Thus, we find that this channel is distillable and all its two-way capacities are given by

$$\mathcal{C}(\eta) = D_2(\eta) = Q_2(\eta) = K(\eta) = -\log_2(1-\eta). \quad (19)$$

Interestingly, this capacity coincides with the maximum discord[41] that can be distributed, since we may write[42] $I_{\mathrm{RC}}(\eta)=D(B|A)$, where the latter is the discord of the (asymptotic) Gaussian Choi matrix $\rho_{\mathcal{E}_\eta}$ (ref. 43). We also prove the strict separation $Q_2(\eta)>Q(\eta)$, where Q is the unassisted quantum capacity[28,29].

Expanding equation (19) at high loss $\eta \simeq 0$, we find

$$\mathcal{C}(\eta) \simeq \eta/\ln 2 \simeq 1.44\eta \,(\text{bits per channel use}), \quad (20)$$

or about η nats per channel use. This completely characterizes the fundamental rate-loss scaling which rules long-distance quantum optical communications in the absence of quantum repeaters. It is important to remark that our work also proves the achievability of this scaling. This is a major advance with respect to existing literature, where previous studies with the squashed entanglement[18] only identified a non-achievable upper bound. In Fig. 6, we compare the scaling of equation (20) with the maximum rates achievable by current QKD protocols.

The capacity in equation (19) is also valid for two-way quantum communication with lossy channels, assuming that η is the maximum transmissivity between the forward and feedback channels. It can also be extended to a multiband lossy channel, for which we write $\mathcal{C}=-\sum_i \log_2(1-\eta_i)$, where η_i are the transmissivities of the various bands or frequency components. For instance, for a multimode telecom fibre with constant transmissivity η and bandwidth W, we have

$$\mathcal{C}=-W\log_2(1-\eta). \quad (21)$$

Finally, note that free-space satellite communications may be modelled as a fading lossy channel, that is, an ensemble of lossy channels $\mathcal{E}_{\eta_i}$ with associated probabilities p_i (ref. 44). In particular, slow fading can be associated with variations of satellite-Earth radial distance[45,46]. For a fading lossy channel $\{\mathcal{E}_{\eta_i}, p_i\}$, we may write

$$\mathcal{C} \le -\sum_i p_i \log_2(1-\eta_i). \tag{22}$$

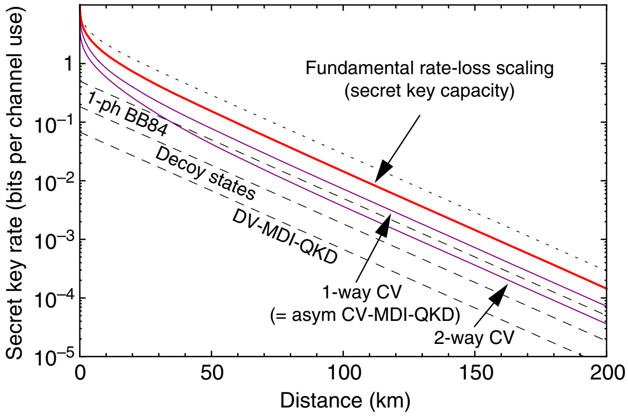

Figure 6 | Ideal performances in QKD. We plot the secret-key rate (bits per channel use) versus Alice–Bob's distance (km) at the loss rate of 0.2 dB per km. The secret-key capacity of the channel (red line) sets the fundamental rate limit for point-to-point QKD in the presence of loss. Compare this capacity with a previous non-achievable upperbound[18] (dotted line). We then show the maximum rates that are potentially achievable by current protocols, assuming infinitely long keys and ideal conditions, such as unit detector efficiencies, zero dark count rates, zero intrinsic error, unit error correction efficiency, zero excess noise (for CVs) and large modulation (for CVs). In the figure, we see that ideal implementations of CV protocols (purple lines) are not so far from the ultimate limit. In particular, we consider: (i) One-way no-switching protocol[63], coinciding with CV-MDI-QKD[20,64] in the most asymmetric configuration (relay approaching Alice[65]). For high loss ($\eta \simeq 0$), the rate scales as $\eta/\ln 4$, which is just 1/2 of the capacity. Same scaling for the one-way switching protocol of ref. 13; (ii) Two-way protocol with coherent states and homodyne detection[66,67] which scales as $\simeq \eta/(4\ln 2)$ for high loss (thermal noise is needed for two-way to beat one-way QKD[66]). For the DV protocols (dashed lines), we consider: BB84 with single-photon sources[4] with rate $\eta/2$; BB84 with weak coherent pulses and decoy states[6] with rate $\eta/(2e)$; and DV-MDI-QKD[68,69] with rate $\eta/(2e^2)$. See Supplementary Note 6 for details on these ideal rates.

Quantum communications with Gaussian noise. The fundamental limit of the lossy channel bounds the two-way capacities of all channels decomposable as $\mathcal{E} = \mathcal{E}'' \circ \mathcal{E}_\eta \circ \mathcal{E}'$ where $\mathcal{E}_\eta$ is a lossy component while $\mathcal{E}'$ and $\mathcal{E}''$ are extra channels. A channel $\mathcal{E}$ of this type is stretchable with resource state $\sigma = \rho_{\mathcal{E}_\eta} \neq \rho_{\mathcal{E}}$ and we may write $\mathcal{C}(\mathcal{E}) \le -\log_2(1-\eta)$. For Gaussian channels, such decompositions are known but we achieve tighter bounds if we directly stretch them using their own Choi matrix.

Let us start from the thermal-loss channel, which can be modelled as a beam splitter with transmissivity η in a thermal background with $\bar{n}$ mean photons. Its action on input quadratures $\hat{\mathbf{x}} = (\hat{q}, \hat{p})$ is given by $\hat{\mathbf{x}} \to \sqrt{\eta}\hat{\mathbf{x}} + \sqrt{1-\eta}\hat{\mathbf{x}}_E$ with E being a thermal mode. This channel is central for microwave communications[47–50] but also important for CV QKD at optical and telecom frequencies, where Gaussian eavesdropping via entangling cloners results into a thermal-loss channel[2].

For an arbitrary thermal-loss channel $\mathcal{E}_{\eta,\bar{n}}$ we apply our reduction method and compute the entanglement flux

$$\Phi(\eta,\bar{n}) \le -\log_2[(1-\eta)\eta^{\bar{n}}] - h(\bar{n}), \tag{23}$$

for $\bar{n} < \eta/(1-\eta)$, while zero otherwise. Here we set

$$h(x) := (x+1)\log_2(x+1) - x\log_2 x. \tag{24}$$

Combining this result with the lower bound given by the reverse coherent information[17], we write the following inequalities for the two-way capacity of this channel

$$-\log_2(1-\eta) - h(\bar{n}) \le \mathcal{C}(\eta,\bar{n}) \le \Phi(\eta,\bar{n}). \tag{25}$$

As shown in Fig. 7a, the two bounds tend to coincide at sufficiently high transmissivity. We clearly retrieve the previous result of the lossy channel for $\bar{n} = 0$.

Another important Gaussian channel is the quantum amplifier. This channel $\mathcal{E}_{g,\bar{n}}$ is described by $\hat{\mathbf{x}} \to \sqrt{g}\hat{\mathbf{x}} + \sqrt{g-1}\hat{\mathbf{x}}_E$, where $g > 1$ is the gain and E is the thermal environment with $\bar{n}$ mean photons. We compute

$$\Phi(g,\bar{n}) \le \log_2\left(\frac{g^{\bar{n}+1}}{g-1}\right) - h(\bar{n}), \tag{26}$$

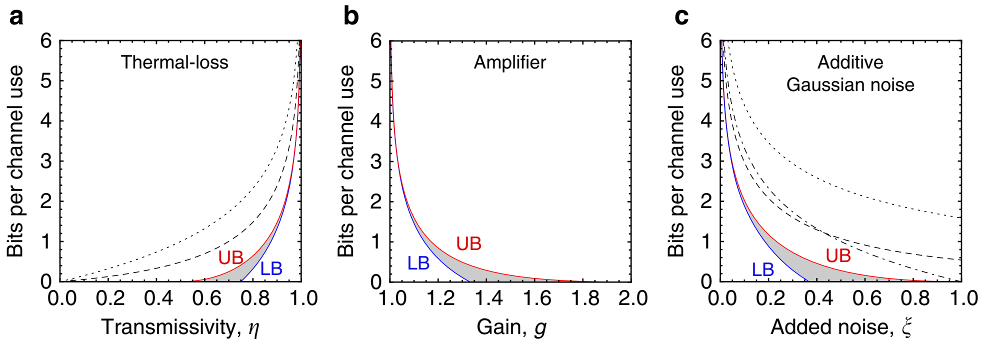

Figure 7 | Two-way capacities for Gaussian channels in terms of the relevant channel parameters. (**a**) Two-way capacity $\mathcal{C}(\eta,\bar{n})$ of the thermal-loss channel as a function of transmissivity η for $\bar{n} = 1$ thermal photon. It is contained in the shadowed area identified by the lower bound (LB) and upper bound (UB) of equation (25). Our upper bound is clearly tighter than those based on the squashed entanglement, computed in ref. 18 (dotted) and ref. 54 (dashed). Note that $\mathcal{C}(\eta,\bar{n}) \simeq -\log_2(1-\eta) - h(\bar{n})$ at high transmissivities. For $\bar{n} = 0$ (lossy channel) the shadowed region shrinks into a single line. (**b**) Two-way capacity $\mathcal{C}(g,\bar{n})$ of the amplifier channel as a function of the gain g for $\bar{n} = 1$ thermal photon. It is contained in the shadowed specified by the bounds in equation (27). For small gains, we have $\mathcal{C}(g,\bar{n}) \simeq \log_2[g/(g-1)] - h(\bar{n})$. For $\bar{n} = 0$ (quantum-limited amplifier) the shadowed region shrinks into a single line. (**c**) Two-way capacity $\mathcal{C}(\xi)$ of the additive-noise Gaussian channel with added noise ξ. It is contained in the shadowed region specified by the bounds in equation (30). For small noise, we have $\mathcal{C}(\xi) \simeq -1/\ln 2 - \log_2 \xi$. Our upper bound is much tighter than those of ref. 18 (dotted), ref. 54 (dashed) and ref. 51 (dot-dashed).

for $\bar{n} < (g-1)^{-1}$, while zero otherwise. Combining this result with the coherent information[51], we get

$$\log_2\left(\frac{g}{g-1}\right) - h(\bar{n}) \leq \mathcal{C}(g,\bar{n}) \leq \Phi(g,\bar{n}), \qquad (27)$$

whose behaviour is plotted in Fig. 7b.

In the absence of thermal noise ($\bar{n} = 0$), the previous channel describes a quantum-limited amplifier $\mathcal{E}_g$, for which the bounds in equation (27) coincide. This channel is therefore distillable and its two-way capacities are

$$\mathcal{C}(g) = D_2(g) = Q_2(g) = K(g) = -\log_2\left(1-g^{-1}\right). \qquad (28)$$

In particular, this proves that $Q_2(g)$ coincides with the unassisted quantum capacity $Q(g)$[51,52]. Note that a gain-2 amplifier can transmit at most 1 qubit per use.

Finally, one of the simplest models of bosonic decoherence is the additive-noise Gaussian channel[2]. This is the direct extension of the classical model of a Gaussian channel to the quantum regime. It can be seen as the action of a random Gaussian displacement over incoming states. In terms of input–output transformations, it is described by $\hat{\mathbf{x}} \to \hat{\mathbf{x}} + (z,z)^T$ where z is a classical Gaussian variable with zero mean and variance $\xi \geq 0$. For this channel $\mathcal{E}_\xi$ we find the entanglement flux

$$\Phi(\xi) \leq \frac{\xi - 1}{\ln 2} - \log_2 \xi, \qquad (29)$$

for $\xi < 1$, while zero otherwise. Including the lower bound given by the coherent information[51], we get

$$-\frac{1}{\ln 2} - \log_2 \xi \leq \mathcal{C}(\xi) \leq \Phi(\xi). \qquad (30)$$

In Fig. 7c, see its behaviour and how the two bounds tend to rapidly coincide for small added noise.

Ultimate limits in qubit communications. We now study the ultimate rates for quantum communication, entanglement distribution and secret-key generation through qubit channels, with generalizations to any finite dimension. For any DV channel $\mathcal{E}$ from dimension d_A to dimension d_B, we may write the dimensionality bound $\mathcal{C}(\mathcal{E}) \leq \min\{\log_2 d_A, \log_2 d_B\}$. This is because we may always decompose the channel into $\mathcal{I} \circ \mathcal{E}$ (or $\mathcal{E} \circ \mathcal{I}$), include $\mathcal{E}$ in Alice's (or Bob's) LOs and stretch the identity map into a Bell state with dimension d_B (or d_A). For DV channels, we may also write the following simplified version of our Theorem 5 (see Methods for proof).

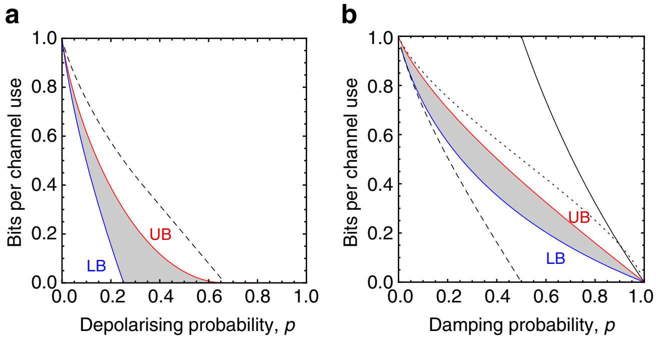

Figure 8 | Two-way capacities of basic qubit channels. (**a**) Two-way capacity of the depolarizing channel $\mathcal{P}_{\text{depol}}$ with arbitrary probability p. It is contained in the shadowed region specified by the bounds in equation (36). We also depict the best-known bound based on the squashed entanglement[54] (dashed). (**b**) Two-way capacity of the amplitude damping channel $\mathcal{E}_{\text{damp}}$ for arbitrary damping probability p. It is contained in the shadowed area identified by the lower bound (LB) of equation (48) and the upper bound (UB) of equation (49). We also depict the bound of equation (47) (upper solid line), which is good only at high dampings; and the bound $C_{\text{A}}(\mathcal{E}_{\text{damp}})/2$ of ref. 54 (dotted line), which is computed from the entanglement-assisted classical capacity C_{A}. Finally, note the separation of the two-way capacity $\mathcal{C}(\mathcal{E}_{\text{damp}})$ from the unassisted quantum capacity $Q(\mathcal{E}_{\text{damp}})$ (dashed line).

Proposition 6: For a Choi-stretchable channel $\mathcal{E}$ in finite dimension, we may write the chain

$$K(\mathcal{E}) = K(\rho_\mathcal{E}) \leq E_{\text{R}}^\infty(\rho_\mathcal{E}) \leq E_{\text{R}}(\rho_\mathcal{E}) = E_{\text{R}}(\mathcal{E}), \qquad (31)$$

where $K(\rho_\mathcal{E})$ is the distillable key of $\rho_\mathcal{E}$.

In the following, we provide our results for DV channels, with technical details available in Supplementary Note 5.

Pauli channels. A general error model for the transmission of qubits is the Pauli channel

$$\mathcal{P}(\rho) = p_0\rho + p_1 X\rho X + p_2 Y\rho Y + p_3 Z\rho Z, \qquad (32)$$

where X, Y, and Z are Pauli operators[1] and $\mathbf{p} := \{p_k\}$ is a probability distribution. It is easy to check that this channel is Choi-stretchable and its Choi matrix is Bell-diagonal. We compute its entanglement flux as

$$\Phi(\mathcal{P}) = 1 - H_2(p_{\max}), \qquad (33)$$

if $p_{\max} := \max\{p_k\} \geq 1/2$, while zero otherwise. Since the channel is unital, we have that $I_{\text{C}}(\mathcal{P}) = I_{\text{RC}}(\mathcal{P}) = 1 - H(\mathbf{p})$, where H is the Shannon entropy. Thus, the two-way capacity of a Pauli channel satisfies

$$1 - H(\mathbf{p}) \leq \mathcal{C}(\mathcal{P}) \leq \Phi(\mathcal{P}). \qquad (34)$$

This can be easily generalized to arbitrary finite dimension (see Supplementary Note 5).

Consider the depolarising channel, which is a Pauli channel shrinking the Bloch sphere. With probability p, an input state becomes the maximally-mixed state

$$\mathcal{P}_{\text{depol}}(\rho) = (1-p)\rho + pI/2. \qquad (35)$$

Setting $\kappa(p) := 1 - H_2\ (3p/4)$, we may then write

$$\kappa(p) - \frac{3p}{4}\log_2 3 \leq \mathcal{C}\left(\mathcal{P}_{\text{depol}}\right) \leq \kappa(p), \qquad (36)$$

for $p \leq 2/3$, while 0 otherwise (Fig. 8a). The result can be extended to any dimension $d \geq 2$. A qudit depolarising channel is defined as in equation (35) up to using the mixed state I/d. Setting $f := p(d^2-1)/d^2$ and $\kappa(d,p) := \log_2 d - H_2(f) - f\log_2(d-1)$, we find

$$\kappa(d,p) - f\log_2(d+1) \leq \mathcal{C}\left(\mathcal{P}_{\text{depol}}\right) \leq \kappa(d,p), \qquad (37)$$

for $p \leq d/(d+1)$, while zero otherwise.

Consider now the dephasing channel. This is a Pauli channel, which deteriorates quantum information without energy decay, as it occurs in spin-spin relaxation or photonic scattering through waveguides. It is defined as

$$\mathcal{P}_{\text{deph}}(\rho) = (1-p)\rho + pZ\rho Z, \qquad (38)$$

where p is the probability of a phase flip. We can easily check that the two bounds of equation (34) coincide, so that this channel is distillable and its two-way capacities are

$$\begin{aligned}\mathcal{C}\left(\mathcal{P}_{\text{deph}}\right) &= D_2\left(\mathcal{P}_{\text{deph}}\right) = Q_2\left(\mathcal{P}_{\text{deph}}\right) \\ &= K\left(\mathcal{P}_{\text{deph}}\right) = 1 - H_2(p).\end{aligned} \qquad (39)$$

Note that this also proves $Q_2\left(\mathcal{P}_{\text{deph}}\right) = Q\left(\mathcal{P}_{\text{deph}}\right)$, where the latter was derived in ref. 53.

For an arbitrary qudit with computational basis $\{|j\rangle\}$, the generalized dephasing channel is defined as

$$\mathcal{P}_{\text{deph}}(\rho) = \sum_{i=0}^{d-1} P_i Z^i \rho \left(Z^{\dagger}\right)^i, \tag{40}$$

where P_i is the probability of i phase flips, with a single flip being $Z|j\rangle = e^{ij2\pi/d}|j\rangle$. This channel is distillable and its two-way capacities are functionals of $\mathbf{P} = \{P_i\}$

$$\mathcal{C}\left(\mathcal{P}_{\text{deph}}\right) = \log_2 d - H(\mathbf{P}). \tag{41}$$

Quantum erasure channel. A simple decoherence model is the erasure channel. This is described by

$$\mathcal{E}_{\text{erase}}(\rho) = (1-p)\rho + p|e\rangle\langle e|, \tag{42}$$

where p is the probability of getting an orthogonal erasure state $|e\rangle$. We already know that $Q_2(\mathcal{E}_{\text{erase}}) = 1-p$ (ref. 12). Therefore, we compute the secret-key capacity.

Following ref. 12, one shows that $D_1\left(\rho_{\mathcal{E}_{\text{erase}}}\right) \geq 1-p$. In fact, suppose that Alice sends halves of EPR states to Bob. A fraction $1-p$ will be perfectly distributed. These good cases can be identified by Bob applying the measurement $\{|e\rangle\langle e|, I - |e\rangle\langle e|\}$ on each output system, and communicating the results back to Alice in a single and final CC. Therefore, they distill at least $1-p$ ebits per copy. It is then easy to check that this channel is Choi-stretchable and we compute $\Phi\left(\rho_{\mathcal{E}_{\text{erase}}}\right) \leq 1-p$. Thus, the erasure channel is distillable and we may write

$$\mathcal{C}(\mathcal{E}_{\text{erase}}) = K(\mathcal{E}_{\text{erase}}) = 1-p. \tag{43}$$

In arbitrary dimension d, the generalized erasure channel is defined as in equation (42), where ρ is now the state of a qudit and the erasure state $|e\rangle$ lives in the extra $d+1$ dimension. We can easily generalize the previous derivations to find that this channel is distillable and

$$K(\mathcal{E}_{\text{erase}}) = (1-p)\log_2 d. \tag{44}$$

Note that the latter result can also be obtained by computing the squashed entanglement of the erasure channel, as shown by the independent derivation of ref. 54.

Amplitude damping channel. Finally, an important model of decoherence in spins or optical cavities is energy dissipation or amplitude damping[55,56]. The action of this channel on a qubit is

$$\mathcal{E}_{\text{damp}}(\rho) = \sum_{i=0,1} A_i \rho A_i^{\dagger}, \tag{45}$$

where $A_0 := |0\rangle\langle 0| + \sqrt{1-p}|1\rangle\langle 1|$, $A_1 := \sqrt{p}|0\rangle\langle 1|$, and p is the damping probability. Note that $\mathcal{E}_{\text{damp}}$ is not teleportation-covariant. However, it is decomposable as

$$\mathcal{E}_{\text{damp}} = \mathcal{E}_{\text{CV}\to\text{DV}} \circ \mathcal{E}_{\eta(p)} \circ \mathcal{E}_{\text{DV}\to\text{CV}}, \tag{46}$$

where $\mathcal{E}_{\text{DV}\to\text{CV}}$ teleports the original qubit into a single-rail bosonic qubit[9]; then, $\mathcal{E}_{\eta(p)}$ is a lossy channel with transmissivity $\eta(p) := 1-p$; and $\mathcal{E}_{\text{CV}\to\text{DV}}$ teleports the single-rail qubit back to the original qubit. Thus, $\mathcal{E}_{\text{damp}}$ is stretchable into the asymptotic Choi matrix of the lossy channel $\mathcal{E}_{\eta(p)}$. This shows that we need a dimension-independent theory even for stretching DV channels.

From Theorem 5 we get $\mathcal{C}\left(\mathcal{E}_{\text{damp}}\right) \leq \Phi\left(\mathcal{E}_{\eta(p)}\right)$, implying

$$\mathcal{C}\left(\mathcal{E}_{\text{damp}}\right) \leq \min\{1, -\log_2 p\}, \tag{47}$$

while the reverse coherent information implies[14]

$$\max_u \{H_2(u) - H_2(up)\} \leq \mathcal{C}\left(\mathcal{E}_{\text{damp}}\right). \tag{48}$$

The bound in equation (47) is simple but only good for strong damping ($p > 0.9$). A shown in Fig. 8b, we find a tighter bound using the squashed entanglement, that is,

$$\mathcal{C}\left(\mathcal{E}_{\text{damp}}\right) \leq H_2\left(\frac{1}{2} - \frac{p}{4}\right) - H_2\left(1 - \frac{p}{4}\right). \tag{49}$$

Discussion

In this work, we have established the ultimate rates for point-to-point quantum communication, entanglement distribution and secret-key generation at any dimension, from qubits to bosonic systems. These limits provide the fundamental benchmarks that only quantum repeaters may surpass. To achieve our results we have designed a general reduction method for adaptive protocols, based on teleportation stretching and the relative entropy of entanglement, suitably extended to quantum channels. This method has allowed us to bound the two-way capacities (Q_2, D_2 and K) with single-letter quantities, establishing exact formulas for bosonic lossy channels, quantum-limited amplifiers, dephasing and erasure channels, after about 20 years since the first studies[12,31].

In particular, we have characterized the fundamental rate-loss scaling which affects any quantum optical communication, setting the ultimate achievable rate for repeaterless QKD at $-\log_2(1-\eta)$ bits per channel use, that is, about 1.44η bits per use at high loss. There are two remarkable aspects to stress about this bound. First, it remains sufficiently tight even when we consider input energy constraints (down to $\simeq 1$ mean photon). Second, it can be reached by using one-way CCs with a maximum cost of just $\log_2(3\pi e) \approx 4.68$ classical bits per channel use; this means that our bound directly provides the throughput in terms of bits per second, once a clock is specified (see Supplementary Note 7 for more details).

Our reduction method is very general and goes well beyond the scope of this work. It has been already used to extend the results to quantum repeaters. Reference 57 has shown how to simplify the most general adaptive protocols of quantum and private communication between two end-points of a repeater chain and, more generally, of an arbitrary multi-hop quantum network, where systems may be routed though single or multiple paths. Depending on the type of routing, the end-to-end capacities are determined by quantum versions of the widest path problem and the max-flow min-cut theorem. More recently, teleportation stretching has been also used to completely simplify adaptive protocols of quantum parameter estimation and quantum channel discrimination[58]. See Supplementary Discussion for a summary of our findings, other follow-up works and further remarks.

Methods

Basics of bosonic systems and Gaussian states. Consider n bosonic modes with quadrature operators $\hat{x} = (\hat{q}_1, \ldots, \hat{q}_n, \hat{p}_1, \ldots, \hat{p}_n)^T$. The latter satisfy the canonical commutation relations[59]

$$\left[\hat{x}, \hat{x}^T\right] = i\Omega, \quad \Omega := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes I_n, \tag{50}$$

with I_n being the $n \times n$ identity matrix. An arbitrary multimode Gaussian state $\rho(u, V)$, with mean value u and covariance matrix (CM) V, can be written as[60]

$$\rho = \frac{\exp\left[-\frac{1}{2}(\hat{x}-u)^T G(\hat{x}-u)\right]}{\det(V + i\Omega/2)^{1/2}}, \tag{51}$$

where the Gibbs matrix G is specified by

$$G = 2i\Omega \coth^{-1}(2Vi\Omega). \tag{52}$$

Using symplectic transformations[2], the CM V can be decomposed into the Williamson's form $\oplus_{k=1}^{n} \nu_k I_2$ where the generic symplectic eigenvalue ν_k satisfies the uncertainty principle $\nu_k \geq 1/2$. Similarly, we may write $\nu_k = \bar{n}_k + 1/2$ where $\bar{n}_k$ are thermal numbers, that is, mean number of photons in each mode. The von

Neumann entropy of a Gaussian state can be easily computed as

$$S(\rho)=\sum_{k=1}^{n} h(\bar{n}_k), \tag{53}$$

where $h(x)$ is given in equation (24).

A two-mode squeezed vacuum (TMSV) state Φ^{μ} is a zero-mean pure Gaussian state with CM

$$V^{\mu}=\begin{pmatrix}\mu & c\\ c & \mu\end{pmatrix}\oplus\begin{pmatrix}\mu & -c\\ -c & \mu\end{pmatrix}, \tag{54}$$

where $c:=\sqrt{\mu^2-1/4}$ and $\mu=\bar{n}+1/2$. Here $\bar{n}$ is the mean photon number of the reduced thermal state associated with each mode A and B. The Wigner function of a TMSV state Φ^{μ} is the Gaussian

$$W[\Phi^{\mu}](x)=\pi^{-2}\exp\left[-\frac{x^T(V^{\mu})^{-1}x}{2}\right], \tag{55}$$

where $x:=(q_A, q_B, p_A, p_B)^T$. For large μ, this function assumes the delta-like expression[25]

$$W[\Phi^{\mu}](x)\to N\,\delta(q_A-q_B)\delta(p_A+p_B), \tag{56}$$

where N is a normalization factor, function of the anti-squeezed quadratures $q_+:=q_A+q_B$ and $p_-:=p_A-p_B$, such that $\int N(q_+,p_-)dq_+dp_-=1$. Thus, the infinite-energy limit of TMSV states $\lim_{\mu}\Phi^{\mu}$ defines the asymptotic CV EPR state Φ, realizing the ideal EPR conditions $\hat{q}_A=\hat{q}_B$ for position and $\hat{p}_A=-\hat{p}_B$ for momentum.

Finally, recall that single-mode Gaussian channels can be put in canonical form[2], so that their action on input quadratures $\hat{x}=(\hat{q},\hat{p})^T$ is

$$\hat{x}\to T\hat{x}+N\hat{x}_E+z, \tag{57}$$

where T and N are diagonal matrices, E is an environmental mode with $\bar{n}_E$ mean photons, and z is a classical Gaussian variable, with zero mean and CM $\xi I\geq 0$.

Relative entropy between Gaussian states. We now provide a simple formula for the relative entropy between two arbitrary Gaussian states $\rho_1(u_1, V_1)$ and $\rho_2(u_2, V_2)$ directly in terms of their statistical moments. Because of this feature, our formula supersedes previous expressions[61,62]. We have the following.

Theorem 7: For two arbitrary multimode Gaussian states, $\rho_1(u_1, V_1)$ and $\rho_2(u_2, V_2)$, the entropic functional

$$\Sigma:=-\mathrm{Tr}\left(\rho_1\log_2\rho_2\right) \tag{58}$$

is given by

$$\Sigma(V_1,V_2,\delta)=\frac{\ln\det\left(V_2+\frac{i\Omega}{2}\right)+\mathrm{Tr}(V_1G_2)+\delta^TG_2\delta}{2\ln 2}, \tag{59}$$

where $\delta:=u_1-u_2$ and $G:=g(V)$ as given in equation (52). As a consequence, the von Neumann entropy of a Gaussian state $\rho(u, V)$ is equal to

$$S(\rho):=-\mathrm{Tr}(\rho\log_2\rho)=\Sigma(V,V,0), \tag{60}$$

and the relative entropy of two Gaussian states $\rho_1(u_1, V_1)$ and $\rho_2(u_2, V_2)$ is given by

$$\begin{aligned}S(\rho_1\|\rho_2):=&\mathrm{Tr}\left[\rho_1\left(\log_2\rho_1-\log_2\rho_2\right)\right]\\ =&-S(\rho_1)-\mathrm{Tr}\left(\rho_1\log_2\rho_2\right)\\ =&-\Sigma(V_1,V_1,0)+\Sigma(V_1,V_2,\delta).\end{aligned} \tag{61}$$

Proof: The starting point is the use of the Gibbs-exponential form for Gaussian states[60] given in equation (51). Start with zero-mean Gaussian states, which can be written as $\rho_i=Z_i^{-1}\exp[-\hat{x}^TG_i\hat{x}/2]$, where $G_i=g(V_i)$is the Gibbs-matrix and $Z_i=\det(V_i+i\Omega/2)^{1/2}$ is the normalization factor (with $i=1, 2$). Then, replacing into the definition of Σ given in equation (58), we find

$$\begin{aligned}(2\ln 2)\Sigma=&2\ln Z_2+\mathrm{Tr}\left(\rho_1\hat{x}^TG_2\hat{x}\right)\\ =&\ln\det(V_2+i\Omega/2)\\ &+\sum_{jk}\mathrm{Tr}\left(\rho_1\hat{x}_j\hat{x}_k\right)G_{2jk}.\end{aligned} \tag{62}$$

Using the commutator $\left\langle\left[\hat{x}_j,\hat{x}_k\right]\right\rangle=i\Omega_{jk}$ and the anticommutator $\left\langle\left\{\hat{x}_j,\hat{x}_k\right\}\right\rangle=2V_{jk}$, we derive

$$\begin{aligned}\sum_{jk}\mathrm{Tr}\left(\rho_1\hat{x}_j\hat{x}_k\right)G_{2jk}=&\mathrm{Tr}\left[\left(V_1+\frac{i\Omega}{2}\right)^TG_2\right]\\ =&\mathrm{Tr}(V_1G_2),\end{aligned} \tag{63}$$

where we also exploit the fact that $\mathrm{Tr}(\Omega G)=0$, because Ω is antisymmetric and G is symmetric (as V).

Let us now extend the formula to non-zero mean values (with difference $\delta=u_1-u_2$). This means to perform the replacement $\hat{x}\to\hat{x}-u_2$, so that

$$\begin{aligned}\mathrm{Tr}\left(\rho_1\hat{x}_j\hat{x}_k\right)\to&\mathrm{Tr}\left[\rho_1\left(\hat{x}_j-u_{2j}\right)\left(\hat{x}_k-u_{2k}\right)\right]\\ =&\mathrm{Tr}\left[\rho_1\left(\hat{x}_j-u_{1j}+\delta_j\right)\left(\hat{x}_k-u_{1k}+\delta_k\right)\right]\\ =&\mathrm{Tr}\left[\rho_1\left(\hat{x}_j-u_{1j}\right)\left(\hat{x}_k-u_{1k}\right)\right]+\delta_j\delta_k.\end{aligned} \tag{64}$$

By replacing this expression in equation (63), we get

$$\sum_{jk}\mathrm{Tr}\left(\rho_1\hat{x}_j\hat{x}_k\right)G_{2jk}\to\mathrm{Tr}(V_1G_2)+\delta^TG_2\delta. \tag{65}$$

Thus, by combining equations (62) and (65), we achieve equation (59). The other equations (60) and (61) are immediate consequences. This completes the proof of Theorem 7.

As discussed in ref. 60, the Gibbs-matrix G becomes singular for a pure state or, more generally, for a mixed state containing vacuum contributions (that is, with some of the symplectic eigenvalues equal to 1/2). In this case the Gibbs-exponential form must be used carefully by making a suitable limit. Since Σ is basis independent, we can perform the calculations in the basis in which V_2, and therefore G_2, is diagonal. In this basis

$$\Sigma=\frac{1}{2}\sum_{k=1}^{n}\sum_{\pm}\alpha_k^{\pm}\log_2(\nu_{2k}\pm 1/2), \tag{66}$$

where $\{\nu_{2k}\}$ is the symplectic spectrum of V_2, and

$$\alpha_k^{\pm}=1\pm\left[(V_1)_{k,k}+(V_1)_{k+n,k+n}\right]. \tag{67}$$

Now, if $\nu_{2k}=1/2$ for some k, then its contribution to the sum in equation (66) is either zero or infinity.

Basics of quantum teleportation. Ideal teleportation exploits an ideal EPR state $\Phi_{AB}=|\Phi\rangle_{AB}\langle\Phi|$ of systems A (for Alice) and B (for Bob). In finite dimension d, this is the maximally entangled Bell state

$$|\Phi\rangle_{AB}:=d^{-1/2}\sum_{i=0}^{d-1}|i\rangle_A|i\rangle_B. \tag{68}$$

In particular, it is the usual Bell state $(|00\rangle+|11\rangle)/\sqrt{2}$ for a qubit. To teleport, we need to apply a Bell detection $\mathcal{B}$ on the input system a and the EPR system A (that is, Alice's part of the EPR state). This detection corresponds to projecting onto a basis of Bell states $|\Phi^k\rangle_{aA}$ where the outcome k takes d^2 values with probabilities $p_k=d^{-2}$.

More precisely, the Bell detection is a positive-operator valued measure with operators

$$M_k=(U_k\otimes I)^{\dagger}\Phi_{aA}(U_k\otimes I), \tag{69}$$

where $\Phi_{aA}:=|\Phi\rangle_{aA}\langle\Phi|$ is the Bell state as in equation (68) and U_k is one of d^2 teleportation unitaries, corresponding to generalized Pauli operators (described below). For any state ρ of the input system a, and outcome k of the Bell detection, the other EPR system B (Bob's part) is projected onto $U_k\rho U_k^{\dagger}$. Once Alice has communicated k to Bob (feed-forward), he applies the correction unitary U_k^{-1} to retrieve the original state ρ on its system B. Note that this process also teleports all correlations that the input system a may have with ancillary systems.

For CV systems ($d\to+\infty$), the ideal EPR source Φ_{AB} can be expressed as a TMSV state Φ^{μ} in the limit of infinite-energy $\mu\to+\infty$. The unitaries U_k are phase-space displacements $D(k)$ with complex amplitude k (ref. 9). The CV Bell detection is also energy-unbounded, corresponding to a projection onto the asymptotic EPR state up to phase-space displacements $D(k)$. To deal with this, we need to consider a finite-energy version of the measurement, defined as a quasi-projection onto displaced versions of the TMSV state Φ^{μ} with finite parameter μ. This defines a positive-operator valued measure $\mathcal{B}^{\mu}$ with operators

$$M_k^{\mu}:=\pi^{-1}[D(-k)\otimes I]\Phi_{aA}^{\mu}[D(k)\otimes I]. \tag{70}$$

Optically, this can be interpreted as applying a balanced beam-splitter followed by two projections, one onto a position-squeezed state and the other onto a momentum-squeezed state (both with finite squeezing). The ideal CV Bell detection $\mathcal{B}$ is reproduced by taking the limit of $\mu\to+\infty$ in equation (70). Thus, CV teleportation must always be interpreted *a la* Braunstein and Kimble[25], so that we first consider finite resources $(\Phi^{\mu},\mathcal{B}^{\mu})$ to compute the μ-dependent output and then we take the limit of large μ.

Teleportation unitaries. Let us characterize the set of teleportation unitaries $\mathbb{U}_d=\{U_k\}$ for a qudit of dimension d. First, let us write k as a multi-index $k=(a, b)$ with $a, b\in\mathbb{Z}_d:=\{0,\ldots,d-1\}$. The teleportation set is therefore composed of d^2 generalized Pauli operators $\mathbb{U}_d=\{U_{ab}\}$, where $U_{ab}:=X^aZ^b$. These are defined by introducing unitary (non-Hermitian) operators

$$X|j\rangle=|j\oplus 1\rangle, Z|j\rangle=\omega^j|j\rangle, \tag{71}$$

where $\oplus$ is the modulo d addition and

$$\omega := \exp(i2\pi/d), \tag{72}$$

so that they satisfy the generalized commutation relation

$$Z^b X^a = \omega^{ab} X^a Z^b. \tag{73}$$

Note that any qudit unitary can be expanded in terms of these generalized Pauli operators. We may construct the set of finite-dimensional displacement operators $D(j,\, a,\, b) := \omega^j X^a Z^b$ with $j, a, b \in \mathbb{Z}_d$ which form the finite-dimensional Weyl–Heisenberg group (or Pauli group). For instance, for a qubit ($d=2$), we have $\mathbb{U}_2 = \{I, X, XZ, Z\}$ and the group $\pm 1 \times \{I,\, X,\, XZ,\, Z\}$. For a CV system ($d = +\infty$), the teleportation set is composed of infinite displacement operators, that is, we have $\mathbb{U}_\infty = \{D(k)\}$, where $D(k)$ is a phase-space displacement operator[2] with complex amplitude k. This set is the infinite-dimensional Weyl–Heisenberg group.

It is important to note that, at any dimension (finite or infinite), the teleportation unitaries satisfy

$$U_k U_\ell = \mathrm{e}^{i\phi(k,l)} U_f, \tag{74}$$

where U_f is another teleportation unitary and $\phi(k, \ell)$ is a phase. In fact, for finite d, let us write k and ℓ as multi-indices, that is, $k = (a,\, b)$ and $\ell = (s, t)$. From $U_{ab} = X^a Z^b = \sum_n \omega^{nb} |n \oplus a\rangle\langle n|$, we see that $U_{ab} U_{st} = \omega^{sb} U_{a\oplus s, b\oplus t}$. Then, for infinite d, we know that the displacement operators satisfy $D(u)D(v) = \mathrm{e}^{uv^* - u^* v} D(u+v)$, for any two complex amplitudes u and v.

Now, let us represent a teleportation unitary as

$$\mathcal{U}_g(\rho) := U_g \rho U_g^\dagger. \tag{75}$$

It is clear that we have $\mathcal{U}_{a,b} \circ \mathcal{U}_{s,t} = \mathcal{U}_{a\oplus s, b\oplus t}$ for DV systems, and $\mathcal{U}_u \circ \mathcal{U}_v = \mathcal{U}_{u+v}$ for CV systems. Therefore $\mathcal{U}_g$ satisfies the group structure

$$\mathcal{U}_g \circ \mathcal{U}_h = \mathcal{U}_{g\cdot h} \quad (g, h \in G), \tag{76}$$

where G is a product of two groups of addition modulo d for DVs, while G is the translation group for CVs. Thus, the (multi-)index of the teleportation unitaries can be taken from the abelian group G.

Teleportation-covariant channels. Let us a give a group representation to the property of teleportation covariance specified by equation (9). Following equation (75), we may express an arbitrary teleportation unitary as $\mathcal{U}_g(\rho) := U_g \rho U_g^\dagger$ where $g \in G$. Calling $\mathcal{V}_g(\rho) := V_g \rho V_g^\dagger$, we see that equation (9) implies

$$\mathcal{V}_g \circ \mathcal{V}_h \circ \mathcal{E} = \mathcal{E} \circ \mathcal{U}_g \circ \mathcal{U}_h = \mathcal{E} \circ \mathcal{U}_{g\cdot h} = \mathcal{V}_{g\cdot h} \circ \mathcal{E}, \tag{77}$$

so that $\mathcal{U}$ and $\mathcal{V}$ are generally different unitary representations of the same abelian group G. Thus, equation (9) can also be written as

$$\mathcal{V}_h^\dagger \circ \mathcal{E} \circ \mathcal{U}_h = \mathcal{E}, \tag{78}$$

for all $h \in G$, where $\mathcal{V}_h^\dagger(\rho) := V_h^\dagger \rho V_h = \mathcal{V}_{h^{-1}}(\rho)$.

The property of equation (9) is certainly satisfied if the channel is covariant with respect to the Weyl–Heisenberg group, describing the teleportation unitaries in both finite- and infinite-dimensional Hilbert spaces. This happens when the channel is dimension-preserving and we may set $V_k = U_{k'}$ for some k' in equation (9). Equivalently, this also means that $\mathcal{U}$ and $\mathcal{V}$ are exactly the same unitary representation in equation (78). We call 'Weyl-covariant' these specific types of tele-covariant channels.

In finite-dimension, a Weyl-covariant channel must necessarily be a Pauli channel. In infinite-dimension, a Weyl-covariant channel commutes with displacements, which is certainly a property of the bosonic Gaussian channels. A simple channel that is tele-covariant but not Weyl-covariant is the erasure channel. This is in fact dimension-altering (since it adds an orthogonal state to the input Hilbert space) and the output correction unitaries to be used in equation (9) have the augmented form $V_k = U_k \oplus I$. Hybrid channels, mapping DVs into CVs or vice versa, cannot be Weyl-covariant but they may be tele-covariant. Finally, the amplitude damping channel is an example of a channel, which is not tele-covariant.

Note that, for a quantum channel in finite dimension, we may easily re-write equation (9) in terms of an equivalent condition for the Choi matrix. In fact, by evaluating the equality in equation (9) on the EPR state $\Phi = |\Phi\rangle\langle\Phi|$ and using the property that $I \otimes U|\Phi\rangle = U^T \otimes I|\Phi\rangle$, one finds

$$\rho_{\mathcal{E}} = \left(U_k^* \otimes V_k\right) \rho_{\mathcal{E}} \left(U_k^T \otimes V_k^\dagger\right). \tag{79}$$

Thus, a finite-dimensional $\mathcal{E}$ is tele-covariant if and only if, for any teleportation unitary U_k, we may write

$$\left[\rho_{\mathcal{E}}, U_k^* \otimes V_k\right] = 0, \tag{80}$$

for another generally different unitary V_k. There are finite-dimensional channels satisfying conditions stronger than equation (80). For Pauli channels, we may write $\left[\rho_{\mathcal{E}}, U_k^* \otimes U_k\right] = 0$ for any k, that is, the Choi matrix is invariant under twirling operations restricted to the generators of the Pauli group $\{U_k\}$. For depolarising channels, we may even write $\left[\rho_{\mathcal{E}}, U^* \otimes U\right] = 0$ for an arbitrary unitary U. This means that the Choi matrix of a depolarising channel is an isotropic state.

LOCC-averaging in teleportation stretching. Consider an arbitrary adaptive protocol described by some fundamental preparation of the local registers $\rho_{\mathbf{a}}^0 \otimes \rho_{\mathbf{b}}^0$ and a sequence of adaptive LOCCs $\mathcal{L} := \{\Lambda_0, \, \dots, \Lambda_n\}$. In general, these LOs may involve measurements. Call u_i the (vectorial) outcome of Alice's and Bob's local measurements performed within the ith adaptive LOCC, so that $\Lambda_i = \Lambda_i^{u_i}$. It is clear that $\Lambda_i^{u_i}$ will be conditioned by measurements and outcomes of all the previous LOCCs, so that a more precise notation will be $\Lambda_{i|i-1, i-2\cdots}^{u_i}$ where the output u_i is achieved with a conditional probability $p(u_i|u_{i-1}, u_{i-2} \, \dots)$. After n transmissions, we have a sequence of outcomes $\mathbf{u} = u_0 \, \dots \, u_n$ with joint probability

$$p(\mathbf{u}) = p(u_0) p(u_1|u_0) \, \dots \, p(u_n|u_{n-1} \, \dots), \tag{81}$$

and a sequence of LOCCs

$$\mathcal{L}(\mathbf{u}) := \left\{\Lambda_0^{u_0}, \Lambda_{1|0}^{u_1}, \, \dots, \Lambda_{n|n-1\dots}^{u_n}\right\}. \tag{82}$$

The mean rate of the protocol is achieved by averaging the output state over all possible outcomes $\mathbf{u}$, which is equivalent to considering the output state generated by the trace-preserving LOCC-sequence $\mathcal{L} := \sum_{\mathbf{u}} \mathcal{L}(\mathbf{u})$.

In fact, suppose that the (normalized) output state $\rho_{\mathbf{ab}}^n(\mathbf{u})$ generated by the conditional $\mathcal{L}(\mathbf{u})$ is epsilon-close to a corresponding target state $\phi_n(\mathbf{u})$ with rate $R_n(\mathbf{u})$. This means that we have $D\left[\rho_{\mathbf{ab}}^n(\mathbf{u}), \phi_n(\mathbf{u})\right] \leq \varepsilon$ in trace distance. The mean rate of the protocol $R_n = \langle R_n(\mathbf{u})\rangle := \sum_{\mathbf{u}} p(\mathbf{u}) R_n(\mathbf{u})$ is associated with the average target state $\phi_n = \langle \phi_n(\mathbf{u})\rangle$. It is easy to show that ϕ_n is approximated by the mean output state $\rho_{\mathbf{ab}}^n = \langle \rho_{\mathbf{ab}}^n(\mathbf{u})\rangle$ generated by $\mathcal{L}$. In fact, by using the joint convexity of the trace distance[1], we may write

$$D(\rho_{\mathbf{ab}}^n, \phi_n) \leq \sum_{\mathbf{u}} p(\mathbf{u}) D\left[\rho_{\mathbf{ab}}^n(\mathbf{u}), \phi_n(\mathbf{u})\right] \leq \varepsilon. \tag{83}$$

Now we show that the LOCC-simulation of a channel $\mathcal{E}$ does not change the average output state $\rho_{\mathbf{ab}}^n$ and this state can be re-organized in a block form. The ith (normalized) conditional output $\rho_{\mathbf{ab}}^i$ can be expressed in terms of the $i-1$th output $\rho_{\mathbf{ab}}^{i-1} = \rho_{\mathbf{a}a_i\mathbf{b}}$ as follows

$$\rho_{\mathbf{ab}}^i(u_i|u_{i-1} \, \dots) = \frac{\Lambda_{i|i-1\cdots}^{u_i} \circ \mathcal{E}\left(\rho_{\mathbf{a}a_i\mathbf{b}}\right)}{p(u_i|u_{i-1} \, \dots)}, \tag{84}$$

where $\mathcal{E}$ is meant as $\mathcal{I}_{\mathbf{a}} \otimes \mathcal{E}_{a_i} \otimes \mathcal{I}_{\mathbf{b}}$ with a_i being the system transmitted. Thus, after n transmissions, the conditional output state is $\rho_{\mathbf{ab}}^n(\mathbf{u}) = p(\mathbf{u})^{-1} \Lambda_{\mathbf{u}}^{\mathcal{E}}(\rho_{\mathbf{a}}^0 \otimes \rho_{\mathbf{b}}^0)$, where

$$\Lambda_{\mathbf{u}}^{\mathcal{E}} := \Lambda_{n|n-1\dots}^{u_n} \circ \mathcal{E} \circ \Lambda_{n-1|n-2\dots}^{u_{n-1}} \circ \cdots \circ \Lambda_{1|0}^{u_1} \circ \mathcal{E} \circ \Lambda_0^{u_0}, \tag{85}$$

and the average output state is given by

$$\rho_{\mathbf{ab}}^n = \sum_{\mathbf{u}} p(\mathbf{u}) \rho_{\mathbf{ab}}^n(\mathbf{u}) = \bar{\Lambda}^{\mathcal{E}}\left(\rho_{\mathbf{a}}^0 \otimes \rho_{\mathbf{b}}^0\right), \tag{86}$$

where $\bar{\Lambda}^{\mathcal{E}} := \sum_{\mathbf{u}} \Lambda_{\mathbf{u}}^{\mathcal{E}}$.

For some LOCC $\mathcal{T}$ and resource state σ, let us write the simulation

$$\mathcal{E}(\rho_{\mathbf{a}a_i\mathbf{b}}) = \mathcal{T}(\rho_{\mathbf{a}a_i\mathbf{b}} \otimes \sigma) = \sum_k \mathcal{T}^k(\rho_{\mathbf{a}a_i\mathbf{b}} \otimes \sigma), \tag{87}$$

where $\mathcal{T}^k(\rho) := (\mathbb{A}_k \otimes \mathbb{B}_k)\rho(\mathbb{A}_k \otimes \mathbb{B}_k)^\dagger$ is Alice and Bob's conditional LOCC with probability $p(k)$. For simplicity we omit other technical labels that may describe independent local measurements or classical channels, because they will also be averaged at the end of the procedure. Let us introduce the vector $\mathbf{k} = k_1 \, \dots \, k_n$ where k_i identifies a conditional LOCC $\mathcal{T}^{k_i}$ associated with the ith transmission. Because the LOCC-simulation of the channel is fixed, we have the factorized probability $p(\mathbf{k}) = p(k_1) \, \dots \, p(k_n)$.

By replacing the simulation in equation (84), we obtain

$$\rho_{\mathbf{ab}}^i(u_i|u_{i-1} \, \dots) = \frac{\Lambda_{i|i-1\cdots}^{u_i} \circ \mathcal{T}\left(\rho_{\mathbf{a}a_i\mathbf{b}} \otimes \sigma\right)}{p(u_i|u_{i-1} \, \dots)}. \tag{88}$$

By iteration, the latter equation yields

$$\rho_{\mathbf{ab}}^n(\mathbf{u}) = p(\mathbf{u})^{-1} \Lambda_{\mathbf{u}}^{\mathcal{T}}\left(\rho_{\mathbf{a}}^0 \otimes \rho_{\mathbf{b}}^0 \otimes \sigma^{\otimes n}\right), \tag{89}$$

where

$$\begin{aligned} \Lambda_{\mathbf{u}}^{\mathcal{T}} :=& \Lambda_{n|n-1\cdots}^{u_n} \circ \mathcal{T} \circ \cdots \circ \mathcal{T} \circ \Lambda_0^{u_0} \\ =& \sum_{\mathbf{k}} p(\mathbf{k}) \Lambda_{n|n-1\cdots}^{u_n} \circ \mathcal{T}^{k_n} \circ \cdots \circ \mathcal{T}^{k_1} \circ \Lambda_0^{u_0}. \end{aligned} \tag{90}$$

Therefore, the average output state of the original protocol may be equivalently expressed in the form

$$\rho_{\mathbf{ab}}^n = \bar{\Lambda}^{\mathcal{T}}\left(\rho_{\mathbf{a}}^0 \otimes \rho_{\mathbf{b}}^0 \otimes \sigma^{\otimes n}\right), \quad \bar{\Lambda}^{\mathcal{T}} := \sum_{\mathbf{u}} \Lambda_{\mathbf{u}}^{\mathcal{T}}. \tag{91}$$

Finally, we may include the preparation $\rho_{\mathbf{a}}^0 \otimes \rho_{\mathbf{b}}^0$ in the LOCC, so that we may write

$$\rho_{\mathbf{ab}}^n = \bar{\Lambda}(\sigma^{\otimes n}). \tag{92}$$

To extend this technical proof to CV systems, we perform the replacement $\sum_{\mathbf{u}} \rightarrow \int d\mathbf{u}$ with the probabilities becoming probability densities. Then, $\mathcal{T}$ and σ may be both asymptotic, that is, defined as infinite-energy limits $\mathcal{T} := \lim_\mu \mathcal{T}^\mu$

and $\sigma := \lim_\mu \sigma^\mu$ from corresponding finite-versions $\mathcal{T}^\mu$ and σ^μ. In this case, we repeat the previous procedure for some μ and then we take the limit on the output state $\rho_{\mathbf{ab}}^{n,\mu}$.

Details on Lemma 3 in relation to teleportation stretching with bosonic channels. For a bosonic channel, the Choi matrix and the ideal Bell detection are both energy-unbounded. Therefore, any Choi-based LOCC simulation of these channels must necessarily be asymptotic. Here we discuss in more detail how an asymptotic channel simulation $(\mathcal{T},\sigma) := \lim_\mu(\mathcal{T}^\mu,\sigma^\mu)$ leads to an asymptotic form of stretching as described in Lemma 3. Any operation or functional applied to $(\mathcal{T},\sigma)$ is implicitly meant to be applied to the finite-energy simulation $(\mathcal{T}^\mu,\sigma^\mu)$, whose output then undergoes the μ-limit.

Consider a bosonic channel $\mathcal{E}$ with asymptotic simulation $(\mathcal{T},\sigma) := \lim_\mu(\mathcal{T}^\mu,\sigma^\mu)$. As depicted in Fig. 9, this means that there is a channel $\mathcal{E}^\mu$ generated by $(\mathcal{T}^\mu,\sigma^\mu)$ such that $\mathcal{E} := \lim_\mu \mathcal{E}^\mu$ in the sense that

$$\|\mathcal{I}\otimes\mathcal{E}(\rho_{aa'}) - \mathcal{I}\otimes\mathcal{E}^\mu(\rho_{aa'})\| \xrightarrow{\mu} 0 \text{ for any } \rho_{aa'}. \tag{93}$$

In other words, for any (energy-bounded) bipartite state $\rho_{aa'}$, whose a'-part is propagated, the original channel output $\rho_{ab} := \mathcal{I}\otimes\mathcal{E}(\rho_{aa'})$ and the simulated channel output $\rho_{ab}^\mu := \mathcal{I}\otimes\mathcal{E}^\mu(\rho_{aa'})$ satisfy the limit

$$\|\rho_{ab}^\mu - \rho_{ab}\| \xrightarrow{\mu} 0. \tag{94}$$

By teleportation stretching, we may equivalently decompose the output state ρ_{ab}^μ into the form

$$\rho_{ab}^\mu = \bar{\Lambda}_\mu(\sigma^\mu), \tag{95}$$

where $\bar{\Lambda}_\mu$ is a trace-preserving LOCC, which is includes both $\mathcal{T}^\mu$ and the preparation of $\rho_{aa'}$ (it is trace-preserving because we implicitly assume that we average over all possible measurements present in the simulation LOCC $\mathcal{T}^\mu$). By taking the limit of $\mu\to+\infty$ in equation (95), the state ρ_{ab}^μ becomes the channel output state ρ_{ab} according to equation (94). Therefore, we have the limit

$$\|\rho_{ab} - \bar{\Lambda}_\mu(\sigma^\mu)\| \xrightarrow{\mu} 0, \tag{96}$$

that we may compactly write as

$$\rho_{ab} = \lim_\mu \bar{\Lambda}_\mu(\sigma^\mu). \tag{97}$$

Note that we may express equation (93) in a different form. In fact, consider the set of energy-constrained bipartite states $\mathcal{D}_N := \{\rho_{aa'}|\mathrm{Tr}(\hat{N}\rho_{aa'}) \leq N\}$, where $\hat{N}$ is the total number operator. Then, for two bosonic channels, $\mathcal{E}_1$ and $\mathcal{E}_2$, we may define the energy-bounded diamond norm

$$\|\mathcal{E}_1 - \mathcal{E}_2\|_{\diamond N} := \sup_{\rho_{aa'}\in\mathcal{D}_N} \|\mathcal{I}\otimes\mathcal{E}_1(\rho_{aa'}) - \mathcal{I}\otimes\mathcal{E}_2(\rho_{aa'})\|. \tag{98}$$

Using the latter definition and the fact that $\mathcal{D}_N$ is a compact set, we have that the pointwise limit in equation (93) implies the following uniform limit

$$\|\mathcal{E} - \mathcal{E}^\mu\|_{\diamond N} \xrightarrow{\mu} 0 \text{ for any } N. \tag{99}$$

The latter expression is useful to generalize the reasoning to the adaptive protocol, with LOCCs applied before and after transmission. Consider the output $\rho_{\mathbf{ab}}^n$ after n adaptive uses of the channel $\mathcal{E}$, and the simulated output $\rho_{\mathbf{ab}}^{n,\mu}$, which is generated by replacing $\mathcal{E}$ with the imperfect channel $\mathcal{E}^\mu$. Explicitly, we may write

$$\rho_{\mathbf{ab}}^n = \Lambda_n\circ\mathcal{E}\circ\Lambda_{n-1}\cdots\circ\Lambda_1\circ\mathcal{E}(\rho_{\mathbf{ab}}^0), \tag{100}$$

with its approximate version

$$\rho_{\mathbf{ab}}^{n,\mu} = \Lambda_n\circ\mathcal{E}^\mu\circ\Lambda_{n-1}\cdots\circ\Lambda_1\circ\mathcal{E}^\mu(\rho_{\mathbf{ab}}^0), \tag{101}$$

where it is understood that $\mathcal{E}$ and $\mathcal{E}^\mu$ are applied to system a_i in the ith transmission, that is, $\mathcal{E} = \mathcal{I}_{\mathbf{a}}\otimes\mathcal{E}_{a_i}\otimes\mathcal{I}_{\mathbf{b}}$.

Assume that the mean photon number of the total register states $\rho_{\mathbf{ab}}^n$ and $\rho_{\mathbf{ab}}^{n,\mu}$ is bounded by some large but yet finite value $N(n)$. For instance, we may consider a sequence $N(n) = N(0) + nt$, where $N(0)$ is the initial photon contribution and t is the channel contribution, which may be negative for energy-decreasing channels (like the thermal-loss channel) or positive for energy-increasing channels (like the quantum amplifier). We then prove

$$\|\rho_{\mathbf{ab}}^n - \rho_{\mathbf{ab}}^{n,\mu}\| \leq \sum_{i=0}^{n-1}\|\mathcal{E}-\mathcal{E}^\mu\|_{\diamond N(i)}. \tag{102}$$

In fact, for $n=2$, we may write

$$\begin{aligned}
&\|\rho_{\mathbf{ab}}^2 - \rho_{\mathbf{ab}}^{2,\mu}\| \\
&= \|\Lambda_2\circ\mathcal{E}\circ\Lambda_1\circ\mathcal{E}(\rho_{\mathbf{ab}}^0) - \Lambda_2\circ\mathcal{E}^\mu\circ\Lambda_1\circ\mathcal{E}^\mu(\rho_{\mathbf{ab}}^0)\| \\
&\overset{(1)}{\leq}\|\mathcal{E}\circ\Lambda_1\circ\mathcal{E}(\rho_{\mathbf{ab}}^0) - \mathcal{E}^\mu\circ\Lambda_1\circ\mathcal{E}^\mu(\rho_{\mathbf{ab}}^0)\| \\
&\overset{(2)}{\leq}\|\mathcal{E}\circ\Lambda_1\circ\mathcal{E}(\rho_{\mathbf{ab}}^0) - \mathcal{E}\circ\Lambda_1\circ\mathcal{E}^\mu(\rho_{\mathbf{ab}}^0)\| \\
&+\|\mathcal{E}\circ\Lambda_1\circ\mathcal{E}^\mu(\rho_{\mathbf{ab}}^0) - \mathcal{E}^\mu\circ\Lambda_1\circ\mathcal{E}^\mu(\rho_{\mathbf{ab}}^0)\| \\
&\overset{(3)}{\leq}\|\mathcal{E}(\rho_{\mathbf{ab}}^0) - \mathcal{E}^\mu(\rho_{\mathbf{ab}}^0)\| \\
&+\|\mathcal{E}[\Lambda_1\circ\mathcal{E}^\mu(\rho_{\mathbf{ab}}^0)] - \mathcal{E}^\mu[\Lambda_1\circ\mathcal{E}^\mu(\rho_{\mathbf{ab}}^0)]\| \\
&\overset{(4)}{\leq}\|\mathcal{E}-\mathcal{E}^\mu\|_{\diamond N(0)} + \|\mathcal{E}-\mathcal{E}^\mu\|_{\diamond N(1)},
\end{aligned} \tag{103}$$

where: (1) we use monotonicity under Λ_2; (2) we use the triangle inequality; (3) we use monotonicity with respect to $\mathcal{E}\circ\Lambda_1$; and (4) we use the definition of equation (98) assuming $a' = a_i$ and the energy bound $N(n)$. Generalization to arbitrary n is just a technicality.

By using equation (99) we may write that, for any bound $N(n)$ and $\varepsilon\geq 0$, there is a sufficiently large μ such that $\|\mathcal{E}-\mathcal{E}^\mu\|_{\diamond N(n)}\leq\varepsilon$, so that equation (102) becomes

$$\|\rho_{\mathbf{ab}}^n - \rho_{\mathbf{ab}}^{n,\mu}\| \leq n\varepsilon. \tag{104}$$

By applying teleportation stretching we derive $\rho_{\mathbf{ab}}^{n,\mu} = \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})$, where $\bar{\Lambda}_\mu$ includes the original LOCCs Λ_i and the teleportation LOCCs $\mathcal{T}^\mu$. Thus, equation (104) implies

$$\|\rho_{\mathbf{ab}}^n - \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})\| \leq n\varepsilon, \tag{105}$$

or, equivalently, $\|\rho_{\mathbf{ab}}^n - \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})\| \xrightarrow{\mu} 0$.

Therefore, given an adaptive protocol with arbitrary register energy, and performed n times through a bosonic channel $\mathcal{E}$ with asymptotic simulation, we may write its output state as the (trace-norm) limit

$$\rho_{\mathbf{ab}}^n = \lim_\mu \bar{\Lambda}_\mu(\sigma^{\mu\otimes n}). \tag{106}$$

This means that we may formally write the asymptotic stretching $\bar{\Lambda}(\sigma^{\otimes n}) := \lim_\mu \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})$ for an asymptotic channel simulation $(\mathcal{T},\sigma) := \lim_\mu(\mathcal{T}^\mu,\sigma^\mu)$.

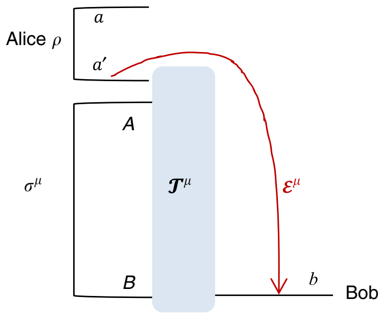

Figure 9 | Asymptotic LOCC simulation of bosonic channels. The finite-energy LOCC simulation $(\mathcal{T}^\mu,\sigma^\mu)$ generates a teleportation channel $\mathcal{E}^\mu$. Assume that $\mathcal{E}^\mu$ defines a target bosonic channel $\mathcal{E}$ according to the pointwise limit in equation (93). Then, we say that the bosonic channel $\mathcal{E}$ has asymptotic simulation $(\mathcal{T},\sigma) := \lim_\mu(\mathcal{T}^\mu,\sigma^\mu)$.

More details on the one-shot REE bound given in Theorem 5. The main steps for proving equation (15) are already given in the main text. Here we provide more details of the formalism for the specific case of bosonic channels, involving asymptotic simulations $(\mathcal{T},\sigma) := \lim_\mu(\mathcal{T}^\mu,\sigma^\mu)$. Given the asymptotic stretching of the output state $\rho_{\mathbf{ab}}^n$ as in equation (106), the simplification of the REE bound $E_{\mathrm{R}}(\rho_{\mathbf{ab}}^n)$ explicitly goes as follows

$$\begin{aligned}
E_{\mathrm{R}}(\rho_{\mathbf{ab}}^n) &= \inf_{\sigma_s} S(\rho_{\mathbf{ab}}^n\|\sigma_s) \\
&\overset{(1)}{\leq} \inf_{\sigma_s^\mu} S\left[\lim_\mu \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})\middle\|\lim_\mu \sigma_s^\mu\right] \\
&\overset{(2)}{\leq} \inf_{\sigma_s^\mu}\liminf_{\mu\to+\infty} S[\bar{\Lambda}_\mu(\sigma^{\mu\otimes n})\|\sigma_s^\mu] \\
&\overset{(3)}{\leq} \inf_{\sigma_s^\mu}\liminf_{\mu\to+\infty} S[\bar{\Lambda}_\mu(\sigma^{\mu\otimes n})\|\bar{\Lambda}_\mu(\sigma_s^\mu)] \\
&\overset{(4)}{\leq} \inf_{\sigma_s^\mu}\liminf_{\mu\to+\infty} S(\sigma^{\mu\otimes n}\|\sigma_s^\mu) \\
&\overset{(5)}{=} E_{\mathrm{R}}(\sigma^{\otimes n}),
\end{aligned} \tag{107}$$

where: (1) σ_s^μ is a generic sequence of separable states that converges in trace norm, that is, such that there is a separable state $\sigma_s := \lim_\mu \sigma_s^\mu$ so that $\|\sigma_s - \sigma_s^\mu\| \xrightarrow{\mu} 0$; (2) we use the lower semi-continuity of the relative entropy[3]; (3) we use that $\bar{\Lambda}_\mu(\sigma_s^\mu)$ are specific types of converging separable sequences within the set of all such sequences; (4) we use the monotonicity of the relative entropy under trace-preserving LOCCs; and (5) we use the definition of REE for asymptotic states given in equation (4).

Thus, from Theorem 1, we may write the following upper bound for the two-way capacity of a bosonic channel

$$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}^{\star}(\mathcal{E}) \leq \lim_{n} n^{-1} E_{\mathrm{R}}(\sigma^{\otimes n}) = E_{\mathrm{R}}^{\infty}(\sigma). \tag{108}$$

The supremum over all adaptive protocols, which defines $E_{\mathrm{R}}^{\star}(\mathcal{E})$ disappears in the right hand side of equation (108). The resulting bound applies to both energy-constrained protocols and the limit of energy-unconstrained protocols. The proof of the further condition $E_{\mathrm{R}}^{\infty}(\sigma) \leq E_{\mathrm{R}}(\sigma)$ in equation (15) comes from the subadditivity of the REE over tensor product states. This subadditivity also holds for a tensor product of asymptotic states; it is proven by restricting the minimization on tensor product sequences $\sigma_s^{\mu \otimes n}$ in the corresponding definition of the REE.

Let us now prove equation (16). The two inequalities in equation (16) are simply obtained by using $\sigma = \rho_{\mathcal{E}}$ for a Choi-stretchable channel (where the Choi matrix is intended to be asymptotic for a bosonic channel). Then we show the equality $E_{\mathrm{R}}(\rho_{\mathcal{E}}) = E_{\mathrm{R}}(\mathcal{E})$. By restricting the optimization in $E_{\mathrm{R}}(\mathcal{E})$ to an input EPR state Φ, we get the direct part $E_{\mathrm{R}}(\mathcal{E}) \geq E_{\mathrm{R}}(\rho_{\mathcal{E}})$ as already noticed in equation (6). For CVs, this means to choose an asymptotic EPR state $\Phi := \lim_{\mu} \Phi^{\mu}$, so that

$$\mathcal{I} \otimes \mathcal{E}(\Phi) := \lim_{\mu} \mathcal{I} \otimes \mathcal{E}(\Phi^{\mu}) = \lim_{\mu} \rho_{\mathcal{E}}^{\mu} := \rho_{\mathcal{E}}, \tag{109}$$

and therefore

$$E_{\mathrm{R}}(\mathcal{E}) \geq E_{\mathrm{R}}(\rho_{\mathcal{E}}) := \inf_{\sigma_s^{\mu}} \liminf_{\mu \to +\infty} S(\rho_{\mathcal{E}}^{\mu} \| \sigma_s^{\mu}). \tag{110}$$

For the converse part, consider first DVs. By applying teleportation stretching to a single use of the channel $\mathcal{E}$, we may write $\mathcal{I} \otimes \mathcal{E}(\rho) = \bar{\Lambda}(\rho_{\mathcal{E}})$ for a trace-preserving LOCC $\bar{\Lambda}$. Then, the monotonicity of the REE leads to

$$E_{\mathrm{R}}(\mathcal{E}) = \sup_{\rho} E_{\mathrm{R}}[\mathcal{I} \otimes \mathcal{E}(\rho)] = \sup_{\rho} E_{\mathrm{R}}\left[\bar{\Lambda}(\rho_{\mathcal{E}})\right] \leq E_{\mathrm{R}}(\rho_{\mathcal{E}}). \tag{111}$$

For CVs, we have an asymptotic stretching $\mathcal{I} \otimes \mathcal{E}(\rho)= \lim_{\mu} \sigma^{\mu}$ where $\sigma^{\mu} := \bar{\Lambda}_{\mu}(\rho_{\mathcal{E}}^{\mu})$. Therefore, we may write

$$\begin{aligned} E_{\mathrm{R}}[\mathcal{I} \otimes \mathcal{E}(\rho)] &= \inf_{\sigma_s^{\mu}} \liminf_{\mu \to +\infty} S(\sigma^{\mu} \| \sigma_s^{\mu}) \\ &\leq \inf_{\sigma_s^{\mu}} \liminf_{\mu \to +\infty} S[\bar{\Lambda}_{\mu}(\rho_{\mathcal{E}}^{\mu}) \| \bar{\Lambda}_{\mu}(\sigma_s^{\mu})] \\ &\leq \inf_{\sigma_s^{\mu}} \liminf_{\mu \to +\infty} S(\rho_{\mathcal{E}}^{\mu} \| \sigma_s^{\mu}) = E_{\mathrm{R}}(\rho_{\mathcal{E}}). \end{aligned} \tag{112}$$

Since this is true for any ρ, it also applies to the supremum and, therefore, to the channel's REE $E_{\mathrm{R}}(\mathcal{E})$.

Proof of Proposition 6 on the one-shot REE bound for DV channels. At finite dimension, we may first use teleportation stretching to derive $K(\mathcal{E}) \leq K(\rho_{\mathcal{E}})$ and then apply any upper bound to the distillable key $K(\rho_{\mathcal{E}})$, among which the REE bound has the best performance. Consider a key generation protocol described by a sequence $\mathcal{L}$ of adaptive LOCCs (implicitly assumed to be averaged). If the protocol is implemented over a Choi-stretchable channel $\mathcal{E}$ in finite dimension d, its stretching allows us to write the output as $\rho_{\mathbf{ab}}^{n} = \bar{\Lambda}(\rho_{\mathcal{E}}^{\otimes n})$ for a trace-preserving LOCC $\bar{\Lambda}$. Since any LOCC-sequence $\mathcal{L}$ is transformed into $\bar{\Lambda}$, any key generation protocol through $\mathcal{E}$ becomes a key distillation protocol over copies of the Choi matrix $\rho_{\mathcal{E}}$. For large n, this means $K(\mathcal{E}) \leq K(\rho_{\mathcal{E}})$.

To derive the opposite inequality, consider Alice sending EPR states through the channel, so that the shared output will be $\rho_{\mathcal{E}}^{\otimes n}$. There exists an optimal LOCC on these states, which reaches the distillable key $K(\rho_{\mathcal{E}})$ for large n. This is a specific key generation protocol over $\mathcal{E}$, so that we may write $K(\rho_{\mathcal{E}}) \leq K(\mathcal{E})$. Thus, for a d-dimensional Choi-stretchable channel, we find

$$K(\mathcal{E}) = K(\rho_{\mathcal{E}}) \leq E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}}), \tag{113}$$

where we also exploit the fact that the distillable key of a DV state is bounded by its regularized REE[27]. It is also clear that $E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}}) \leq E_{\mathrm{R}}(\rho_{\mathcal{E}}) = E_{\mathrm{R}}(\mathcal{E})$, where the latter equality is demonstrated in the proof of Theorem 5.

Note that $K(\mathcal{E}) = K(\rho_{\mathcal{E}})$ cannot be directly written for a bosonic channel, because its Choi matrix $\rho_{\mathcal{E}}$ is energy-unbounded, so that its distillable key $K(\rho_{\mathcal{E}})$ is not well-defined. By contrast, we know how to extend $E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}})$ to bosonic channels and show $K(\mathcal{E}) \leq E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}})$ at any dimension: This is the more general procedure of Theorem 5, which first exploits the general REE bound $K(\mathcal{E}) \leq E_{\mathrm{R}}^{\star}(\mathcal{E})$ and then simplifies $E_{\mathrm{R}}^{\star}(\mathcal{E}) \leq E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}})$ by means of teleportation stretching at any dimension.

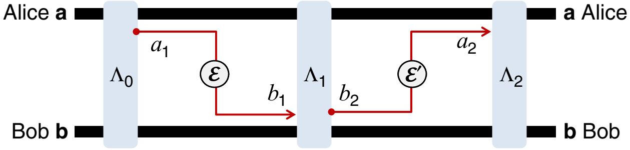

Figure 10 | Adaptive protocol for two-way quantum or private communication. The protocol employs a forward channel $\mathcal{E}$ and backward channel $\mathcal{E}'$. Transmissions are alternated with adaptive LOCCs $\mathcal{L} = \{\Lambda_0, \Lambda_1, \Lambda_2, \ldots\}$.

Two-way quantum communication. Our method can be extended to more complex forms of quantum communication. In fact, our weak converse theorem can be applied to any scenario where two parties produce an output state by means of an adaptive protocol. All the details of the protocol are contained in the LOCCs $\mathcal{L}$ which are collapsed into $\bar{\Lambda}$ by teleportation stretching and then discarded using the REE.

Consider the scenario where Alice and Bob send systems to each other by choosing between two possible channels, $\mathcal{E}$ (forward) or $\mathcal{E}'$ (backward), and performing adaptive LOCC after each single transmission (see also Fig. 10). The capacity $\mathcal{C}(\mathcal{E}, \mathcal{E}')$ is defined as the maximum number of target bits distributed per individual transmission, by using one of the two channels $\mathcal{E}$ and $\mathcal{E}'$, and assuming LOs assisted by unlimited two-way CCs.

In general, the feedback transmission may occur a fraction p of the rounds, with associated capacity

$$\mathcal{C}(p, \mathcal{E}, \mathcal{E}') \geq (1-p)\mathcal{C}(\mathcal{E}) + p\mathcal{C}(\mathcal{E}'). \tag{114}$$

The lower bound is a convex combination of the individual capacities of the two channels, which is achievable by using independent LOCC-sequences for the two channels.

Assume that $(\mathcal{E}, \mathcal{E}')$ are stretchable into the pair of resource states (σ, σ'). Then, we can stretch the protocol and decompose the output state as

$$\rho_{\mathbf{ab}}^{n} = \bar{\Lambda}\left[\sigma^{\otimes n(1-p)} \otimes \sigma'^{\otimes np}\right], \tag{115}$$

where the tensor exponents $n(1-p)$ and np are integers for suitably large n (it is implicitly understood that we consider suitable limits in the bosonic case). Using the monotonicity of the REE under trace-preserving LOCCs and its subadditivity over tensor products, we write

$$\begin{aligned} E_{\mathrm{R}}(\rho_{\mathbf{ab}}^{n}) &\leq E_{\mathrm{R}}\left[\sigma^{\otimes n(1-p)} \otimes \sigma'^{\otimes np}\right] \\ &\leq n(1-p)E_{\mathrm{R}}(\sigma) + npE_{\mathrm{R}}(\sigma'). \end{aligned} \tag{116}$$

As previously said, our weak converse theorem can be applied to any adaptive protocol where two parties finally share a bipartite state $\rho_{\mathbf{ab}}^{n}$. Thus, we may write

$$\begin{aligned} \mathcal{C}(p, \mathcal{E}, \mathcal{E}') &\leq \sup_{\mathcal{L}} \lim_{n \to +\infty} \frac{E_{\mathrm{R}}(\rho_{\mathbf{ab}}^{n})}{n} \\ &\leq (1-p)E_{\mathrm{R}}(\sigma) + pE_{\mathrm{R}}(\sigma'). \end{aligned} \tag{117}$$

From equations (114) and (117), we find that $\mathcal{C}(\mathcal{E}, \mathcal{E}')= \max_{p}\mathcal{C}(p, \mathcal{E}, \mathcal{E}')$ must satisfy

$$\max\{\mathcal{C}(\mathcal{E}), \mathcal{C}(\mathcal{E}')\} \leq \mathcal{C}(\mathcal{E}, \mathcal{E}') \leq \max\{E_{\mathrm{R}}(\sigma), E_{\mathrm{R}}(\sigma')\}. \tag{118}$$

For Choi-stretchable channels, this means

$$\max\{\mathcal{C}(\mathcal{E}), \mathcal{C}(\mathcal{E}')\} \leq \mathcal{C}(\mathcal{E}, \mathcal{E}') \leq \max\{\Phi(\mathcal{E}), \Phi(\mathcal{E}')\}. \tag{119}$$

In particular, if the two channels are distillable, that is, $\mathcal{C}(\mathcal{E}) = \Phi(\mathcal{E})$ and $\mathcal{C}(\mathcal{E}') = \Phi(\mathcal{E}')$, then we may write

$$\mathcal{C}(\mathcal{E}, \mathcal{E}')= \max\{\mathcal{C}(\mathcal{E}), \mathcal{C}(\mathcal{E}')\}, \tag{120}$$

and the optimal strategy (value of p) corresponds to using the channel with maximum capacity.

Note that we may also consider a two-way quantum communication protocol where the forward and backward transmissions occur simultaneously, and correspondingly define a capacity that quantifies the maximum number of target bits which are distributed in each double communication, forward and backward (instead of each single transmission, forward or backward). However, this case can be considered as a double-band quantum channel.

Multiband quantum channel. Consider the communication scenario where Alice and Bob can exploit a multiband quantum channel, that is, a quantum channel whose single use involves the simultaneous transmission of m distinct systems. In practice, this channel $\mathcal{E}_{\mathrm{mb}}$ is represented by a set of m independent channels or bands $\{\mathcal{E}_1, \ldots, \mathcal{E}_m\}$, that is, it can be written as

$$\mathcal{E}_{\mathrm{mb}} = \otimes_{i=1}^{m} \mathcal{E}_i. \tag{121}$$

For instance, the bands may be bosonic Gaussian channels associated with difference frequencies.

In this case, the adaptive protocol is modified in such a way that each (multiband) transmission involves Alice simultaneously sending m quantum systems to Bob. These m input systems may be in a generally entangled state, which may also involve correlations with the remaining systems in Alice's register. Before and after each multiband transmission, the parties perform adaptive LOCCs on their local registers $\mathbf{a}$ and $\mathbf{b}$. The multiband protocol is therefore characterized by a LOCC sequence $\mathcal{L} = \{\Lambda_0, \ldots, \Lambda_n\}$ after n transmissions.

The definition of the generic two-way capacity is immediately extended to a multiband channel. This capacity quantifies the maximum number of target bits that are distributed (in parallel) for each multiband transmission by means of adaptive protocols. It must satisfy

$$\mathcal{C}(\mathcal{E}_{\mathrm{mb}}) \geq \sum_{i=1}^{m} \mathcal{C}(\mathcal{E}_i), \tag{122}$$

where the lower bound is the sum of the two-way capacities of the single bands $\mathcal{E}_i$. This lower bound is obtained by using adaptive LOCCs that are independent between different $\mathcal{E}_i$, and considering an output state of the form $\otimes_i \rho_{\mathbf{ab}}^{n,i}$ where $\rho_{\mathbf{ab}}^{n,i}$ is the output associated with $\mathcal{E}_i$.

Now consider an adaptive protocol performed over a multiband channel, whose m bands $\{\mathcal{E}_i\}$ are stretchable into m resources states $\{\sigma_i\}$. By teleportation stretching, we find that Alice and Bob's output state can be decomposed in the form

$$\rho_{\mathbf{ab}}^{n} = \bar{\Lambda}\left(\otimes_{i=1}^{m} \sigma_i^{\otimes n}\right). \tag{123}$$

(it is understood that the formulation is asymptotic for bosonic channels). This previous decomposition leads to

$$E_{\mathrm{R}}\left(\rho_{\mathbf{ab}}^{n}\right) \leq \sum_{i=1}^{m} E_{\mathrm{R}}\left(\sigma_i^{\otimes n}\right). \tag{124}$$

Using our weak converse theorem, we can then write

$$\begin{aligned} \mathcal{C}(\mathcal{E}_{\mathrm{mb}}) &\leq \sup_{\mathcal{L}} \underset{n\to+\infty}{\lim} \frac{E_{\mathrm{R}}\left(\rho_{\mathbf{ab}}^{n}\right)}{n} \\ &\leq \sum_{i=1}^{m} E_{\mathrm{R}}^{\infty}(\sigma_i) \leq \sum_{i=1}^{m} E_{\mathrm{R}}(\sigma_i). \end{aligned} \tag{125}$$

Combining equations (122) and (125) we may then write

$$\sum_{i=1}^{m} \mathcal{C}(\mathcal{E}_i) \leq \mathcal{C}(\mathcal{E}_{\mathrm{mb}}) \leq \sum_{i=1}^{m} E_{\mathrm{R}}(\sigma_i). \tag{126}$$

For Choi-stretchable bands, this means

$$\sum_{i=1}^{m} \mathcal{C}(\mathcal{E}_i) \leq \mathcal{C}(\mathcal{E}_{\mathrm{mb}}) \leq \sum_{i=1}^{m} \Phi(\mathcal{E}_i). \tag{127}$$

Finally, if the bands are distillable, that is, $\mathcal{C}(\mathcal{E}_i) = \Phi(\mathcal{E}_i)$, then we find the additive result

$$\mathcal{C}(\mathcal{E}_{\mathrm{mb}}) = \sum_{i=1}^{m} \mathcal{C}(\mathcal{E}_i). \tag{128}$$

Code availability. Source codes of the plots are available from the authors on request.

Data availability. No relevant research data were generated in this study.

References

1. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
2. Weedbrook, C. *et al.* Gaussian quantum information. *Rev. Mod. Phys.* **84,** 621–669 (2012).
3. Holevo, A. in *Quantum Systems, Channels, Information: A Mathematical Introduction* (De Gruyter, 2012).
4. Bennett, C. H. & Brassard, G. in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 175–179 (Bangalore, India, 1984).
5. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145–196 (2002).
6. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
7. Kimble, H. J. The quantum internet. *Nature* **453,** 1023–1030 (2008).
8. Pirandola, S. & Braunstein, S. L. Unite to build a quantum internet. *Nature* **532,** 169–171 (2016).
9. Pirandola, S. *et al.* Advances in quantum teleportation. *Nat. Photon.* **9,** 641–652 (2015).
10. Andersen, U. L., Neergaard-Nielsen, J. S., van Loock, P. & Furusawa, A. Hybrid discrete- and continuous-variable quantum information. *Nat. Phys.* **11,** 713–719 (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. Bennett, C. H., DiVincenzo, D. P. & Smolin, J. A. Capacities of quantum erasure channels. *Phys. Rev. Lett.* **78,** 3217–3220 (1997).
13. Grosshans, F. *et al.* Quantum key distribution using gaussian-modulated coherent states. *Nature* **421,** 238–241 (2003).
14. Garca-Patrón, R., Pirandola, S., Lloyd, S. & Shapiro, J. H. Reverse coherent information. *Phys. Rev. Lett.* **102,** 210501 (2009).
15. Devetak, I. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Info. Theory* **51,** 44–55 (2005).
16. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A* **461,** 207–235 (2005).
17. 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).
18. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5,** 5235 (2014).
19. Christandl, M. *The Structure of Bipartite Quantum States: Insights from Group Theory and Cryptography* (PhD thesis, University of Cambridge, 2006).
20. Pirandola, S. *et al.* High-rate measurement-device-independent quantum cryptography. *Nat. Photon.* **9,** 397–402 (2015).
21. Vedral, V., Plenio, M. B., Rippin, M. A. & Knight, P. L. Quantifying Entanglement. *Phys. Rev. Lett.* **78,** 2275–2279 (1997).
22. Vedral, V. & Plenio, M. B. Entanglement measures and purification procedures. *Phys. Rev. A* **57,** 1619–1633 (1998).
23. Vedral, V. The role of relative entropy in quantum information theory. *Rev. Mod. Phys.* **74,** 197–234 (2002).
24. Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70,** 1895–1899 (1993).
25. Braunstein, S. L. & Kimble, H. J. Teleportation of continuous quantum variables. *Phys. Rev. Lett.* **80,** 869–872 (1998).
26. Braunstein, S. L., D'Ariano, G. M., Milburn, G. J. & Sacchi, M. F. Universal teleportation with a twist. *Phys. Rev. Lett.* **84,** 3486–3489 (2000).
27. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. Secure key from bound entanglement. *Phys. Rev. Lett.* **94,** 160502 (2005).
28. Schumacher, B. & Nielsen, M. A. Quantum data processing and error correction. *Phys. Rev. A* **54,** 2629–2635 (1996).
29. Lloyd, S. Capacity of the noisy quantum channel. *Phys. Rev. A* **55,** 1613–1622 (1997).
30. Christiandl, M., Schuch, N. & Winter, A. Entanglement of the antisymmetric state. *Commun. Math. Phys.* **311,** 397–422 (2012).
31. 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).
32. Horodecki, M., Horodecki, P. & Horodecki, R. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A* **99,** 1888–1898 (1999).
33. Bowen, G. & Bose, S. Teleportation as a depolarizing quantum channel, relative entropy and classical capacity. *Phys. Rev. Lett.* **87,** 267901 (2001).
34. Albeverio, S., Fei, S.-M. & Yang, W.-L. Optimal teleportation based on Bell measurements. *Phys. Rev. A* **66,** 012301 (2002).
35. Müller-Hermes, A. *Transposition in Quantum Information Theory* (MSc Thesis, Technische Universität München, 2012).
36. Leung, D. & Matthews, W. On the power of ppt-preserving and nonsignalling codes. *IEEE Trans. Inf. Theory* **61,** 4486–4499 (2015).
37. Werner, R. F. All teleportation and dense coding schemes. *J. Phys. A* **34,** 7081–7094 (2001).
38. Niset, J., Fiurasek, J. & Cerf, N. J. No-go theorem for Gaussian quantum error correction. *Phys. Rev. Lett.* **102,** 120501 (2009).
39. Ji, Z., Wang, G., Duan, R., Feng, Y. & Ying, M. Parameter estimation of quantum channels. *IEEE Trans. Inform. Theory* **54,** 5172–5185 (2008).
40. Nielsen, M. A. & Chuang, I. L. Programmable quantum gate arrays. *Phys. Rev. Lett.* **79,** 321–324 (1997).
41. Modi, K. *et al.* The classical-quantum boundary for correlations: discord and related measures. *Rev. Mod. Phys.* **84,** 1655–1707 (2012).
42. Pirandola, S. Quantum discord as a resource for quantum cryptography. *Sci. Rep.* **4,** 6956 (2014).
43. Pirandola, S., Spedalieri, G., Braunstein, S. L., Cerf, N. J. & Lloyd, S. Optimality of Gaussian discord. *Phys. Rev. Lett.* **113,** 140405 (2014).
44. Hosseinidehaj, N. & Malaney, R. Gaussian entanglement distribution via satellite. *Phys. Rev. A* **91,** 022304 (2015).
45. Vallone, G. *et al.* Experimental satellite quantum communications. *Phys. Rev. Lett.* **115,** 040502 (2015).
46. Dequal, D. *et al.* Experimental single-photon exchange along a space link of 7,000 km. *Phys. Rev. A* **93,** 010301 (R) (2016).
47. Usenko, V. C. & Filip, R. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **81,** 022318 (2010).
48. Weedbrook, C. *et al.* Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **105,** 110501 (2010).
49. Weedbrook, C. *et al.* Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **86,** 022318 (2012).
50. Weedbrook, C., Ottaviani, C. & Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **89,** 012309 (2014).
51. Holevo, A. S. & Werner, R. F. Evaluating capacities of bosonic Gaussian channels. *Phys. Rev. A* **63,** 032312 (2001).
52. Wolf, M. M., Pérez-Garca, D. & Giedke, G. Quantum capacities of bosonic channels. *Phys. Rev. Lett.* **98,** 130501 (2007).

53. Devetak, I. & Shor, P. W. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Commun. Math. Phys.* **256,** 287–303 (2005).
54. Goodenough, K., Elkouss, D. & Wehner, S. Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels. Preprint at https://arxiv.org/abs/1511.08710v1 (2015).
55. Bose, S. Quantum communication through an Unmodulated Spin Chain. *Phys. Rev. Lett.* **20,** 207901 (2003).
56. Bose, S., Bayat, A., Sodano, P., Banchi, L. & Verrucchi, P. in *Quantum State Transfer and Network Engineering* 1–37 (Springer, 2014).
57. Pirandola, S. Capacities of repeater-assisted quantum communications. Preprint at https://arxiv.org/abs/1601.00966 (2016).
58. Pirandola, S. & Lupo, C. Ultimate precision of adaptive noise estimation. *Phys. Rev. Lett.* **118,** 100502 (2017).
59. Dutta, A. B., Mukunda, N. & Simon, R. The real symplectic groups in quantum mechanics and optics. *Pramana* **45,** 471–497 (1995).
60. Banchi, L., Braunstein, S. L. & Pirandola, S. Quantum fidelity for arbitrary Gaussian states. *Phys. Rev. Lett.* **115,** 260501 (2015).
61. Chen, X. Y. Gaussian relative entropy of entanglement. *Phys. Rev. A* **71,** 062320 (2005).
62. Scheel, S. & Welsch, D.-G. Entanglement generation and degradation by passive optical devices. *Phys. Rev. A* **64,** 063811 (2001).
63. Weedbrook, C. *et al.* Quantum cryptography without switching. *Phys. Rev. Lett.* **93,** 170504 (2004).
64. Ottaviani, C., Spedalieri, G., Braunstein, S. L. & Pirandola, S. Continuous-variable quantum cryptography with an untrusted relay: detailed security analysis of the symmetric configuration. *Phys. Rev. A* **91,** 022320 (2015).
65. Spedalieri, G. *et al.* in *Proceedings of SPIE Security + Defence 2015 Conference on Quantum Information Science and Technology* 9648-47 (Toulouse, France, 2015).
66. Pirandola, S., Mancini, S., Lloyd, S. & Braunstein, S. L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **4,** 726–730 (2008).
67. Ottaviani, C. & Pirandola, S. General immunity and superadditivity of two-way Gaussian quantum cryptography. *Sci. Rep.* **6,** 22225 (2016).
68. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108,** 130502 (2012).
69. Lo, H.-K., Curty, M. & Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).

Acknowledgements

We acknowledge support from the EPSRC via the 'UK Quantum Communications Hub' (EP/M013472/1) and 'qDATA' (EP/L011298/1), and from the ERC (Starting Grant 308253 PACOMANEDIA). In alphabetic order we would like to thank G. Adesso, S. Bose, S.L. Braunstein, M. Christandl, T.P.W. Cope, R. Demkowicz-Dobrzanski, K. Goodenough, F. Grosshans, S. Guha, M. Horodecki, L. Jiang, J. Kolodynski, S. Lloyd, C. Lupo, L. Maccone, S. Mancini, A. Müller-Hermes, B. Schumacher, G. Spedalieri, G. Vallone, M. Westmoreland, M.M. Wilde and A. Winter.

Author contributions

S.P. designed the general methodology, which reduces the study of adaptive protocols to single-letter bounds, by devising the technique of teleportation stretching at any dimension and showing its combination with the channel's relative entropy of entanglement; S.P. proved the theorems, propositions and lemmas (with the exception of Theorem 7); S.P. also derived the analytical results for the bosonic Gaussian channels and wrote the manuscript. R.L. contributed to investigate bosonic channels and derived the analytical bounds for the discrete-variable channels, besides studying the classical communication cost. C.O. analysed the ideal rates of current QKD protocols and performed numerical simulations. L.B. proved the general formula for the relative entropy of Gaussian states (Theorem 7), contributed to refine mathematical aspects of teleportation covariance and to improve the bounds for the discrete-variable channels. All the authors checked the manuscript for accuracy.

Additional information

Supplementary Information accompanies this paper at http://www.nature.com/naturecommunications

Competing interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Pirandola, S. *et al.* Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8,** 15043 doi: 10.1038/ncomms15043 (2017).

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