COMMUNICATIONS PHYSICS

ARTICLE

https://doi.org/10.1038/s42005-019-0147-3 OPEN

End-to-end capacities of a quantum communication network

Stefano Pirandola [1,2]

In quantum mechanics, a fundamental law prevents quantum communications to simultaneously achieve high rates and long distances. This limitation is well known for point-to-point protocols, where two parties are directly connected by a quantum channel, but not yet fully understood in protocols with quantum repeaters. Here we solve this problem bounding the ultimate rates for transmitting quantum information, entanglement and secret keys via quantum repeaters. We derive single-letter upper bounds for the end-to-end capacities achievable by the most general (adaptive) protocols of quantum and private communication, from a single repeater chain to an arbitrarily complex quantum network, where systems may be routed through single or multiple paths. We analytically establish these capacities under fundamental noise models, including bosonic loss which is the most important for optical communications. In this way, our results provide the ultimate benchmarks for testing the optimal performance of repeater-assisted quantum communications.

[1] Department of Computer Science, University of York, York YO10 5GH, UK. [2] Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA. Correspondence and requests for materials should be addressed to S.P. (email: stefano.pirandola@york.ac.uk)

Today quantum technologies are being developed at a rapid pace[1–4]. In this scenario, quantum communications are very advanced, with the development and implementation of a number of point-to-point protocols of quantum key distribution (QKD)[5], based on discrete variable (DV) systems[6–8], such as qubits, or continuous variable (CV) systems, such as bosonic modes[9,10]. Recently, we have also witnessed the deployment of high-rate optical-based secure quantum networks[11,12]. These are advantageous not only for their multiple-user architecture but also because they may overcome the fundamental limitations that are associated with point-to-point protocols of quantum and private communication.

After a long series of studies that started back in 2009 with the introduction of the reverse coherent information of a bosonic channel[13,14], ref. [15] finally showed that the maximum rate at which two remote parties can distribute quantum bits (qubits), entanglement bits (ebits), or secret bits over a lossy channel (e.g., an optical fiber) is equal to $-\log_2(1-\eta)$, where η is the channel's transmissivity. This limit is the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound[15] and cannot be surpassed even by the most powerful strategies that exploit arbitrary local operations (LOs) assisted by two-way classical communication (CC), also known as adaptive LOCCs[16].

To beat the PLOB bound, we need to insert a quantum repeater[17] in the communication line. In information theory[18–21], a repeater or relay is any middle node helping the communication between two end-parties. This definition is extended to quantum information theory, where quantum repeaters are middle nodes equipped with both classical and quantum operations, and may be arranged to compose linear chains or more general networks. In general, they do not need to have quantum memories (e.g., see ref. [22]) even though these are generally required for guaranteeing an optimal performance.

In all the ideal repeater-assisted scenarios, where we can beat the PLOB bound, it is fundamental to determine the maximum rates that are achievable by two end-users, i.e., to determine their end-to-end capacities for transmitting qubits, distributing ebits, and generating secret keys. Finding these capacities not only is important to establish the boundaries of quantum network communications but also to benchmark practical implementations, so as to check how far prototypes of quantum repeaters are from the ultimate theoretical performance.

Here we address this fundamental problem. By combining methods from quantum information theory[6–10] and classical networks[18–21], we derive tight single-letter upper bounds for the end-to-end quantum and private capacities of repeater chains and, more generally, quantum networks connected by arbitrary quantum channels (these channels and the dimension of the quantum systems they transmit may generally vary across the network). More importantly, we establish exact formulas for these capacities under fundamental noise models for both DV and CV systems, including dephasing, erasure, quantum-limited amplification, and bosonic loss which is the most important for quantum optical communications. Depending on the routing in the quantum network (single- or multi-path), optimal strategies are found by solving the widest path[23–25] or the maximum flow problem[26–29] suitably extended to the quantum communication setting.

Our results and analytical formulas allow one to assess the rate performance of quantum repeaters and quantum communication networks with respect to the ultimate limits imposed by the laws of quantum mechanics.

Results

Ultimate limits of repeater chains. Consider Alice **a** and Bob **b** at the two ends of a linear chain of N quantum repeaters, labeled by $\mathbf{r}_1, \ldots, \mathbf{r}_N$. Each point has a local register of quantum systems which may be augmented with incoming systems or depleted by outgoing ones. As also depicted in Fig. 1, the chain is connected by $N+1$ quantum channels $\{\mathcal{E}_i\} = \{\mathcal{E}_0, \ldots, \mathcal{E}_i, \ldots, \mathcal{E}_N\}$ through which systems are sequentially transmitted. This means that Alice transmits a system to repeater $\mathbf{r}_1$, which then relays the system to repeater $\mathbf{r}_2$, and so on, until Bob is reached.

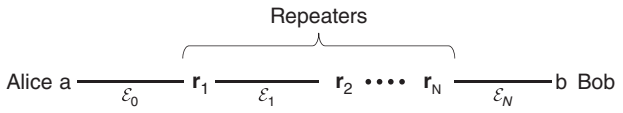

Fig. 1 Linear chain of N quantum repeaters $\mathbf{r}_1, \ldots, \mathbf{r}_N$ between the two end-users, Alice $\mathbf{a} := \mathbf{r}_0$ and Bob $\mathbf{b} := \mathbf{r}_{N+1}$. The chain is connected by $N+1$ quantum channels $\{\mathcal{E}_i\}$

Note that, in general, we may also have opposite directions for some of the quantum channels, so that they transmit systems towards Alice; e.g., we may have a middle relay receiving systems from both Alice and Bob. For this reason, we generally consider the "exchange" of a quantum system between two points by either forward or backward transmission. Under the assistance of two-way CCs, the optimal transmission of quantum information is related to the optimal distribution of entanglement followed by teleportation, so that it does not depend on the physical direction of the quantum channel but rather on the direction of the teleportation protocol.

In a single end-to-end transmission or use of the chain, all the channels are used exactly once. Assume that the end-points aim to share target bits, which may be ebits or private bits[30,31]. The most general quantum distribution protocol $\mathcal{P}_{\text{chain}}$ involves transmissions which are interleaved by adaptive LOCCs among all parties, i.e., LOs assisted by two-way CCs among end-points and repeaters. In other words, before and after each transmission between two nodes, there is a session of LOCCs where all the nodes update and optimize their registers.

After n adaptive uses of the chain, the end-points share an output state $\rho_{\mathbf{ab}}^n$ with nR_n target bits. By optimizing the asymptotic rate $\lim_n R_n$ over all protocols $\mathcal{P}_{\text{chain}}$, we define the generic two-way capacity of the chain $\mathcal{C}(\{\mathcal{E}_i\})$. If the target are ebits, the repeater-assisted capacity $\mathcal{C}$ is an entanglement-distribution capacity D_2. The latter coincides with a quantum capacity Q_2, because distributing an ebit is equivalent to transmitting a qubit if we assume two-way CCs. If the target are private bits, $\mathcal{C}$ is a secret-key capacity $K \geq D_2$ (with the inequality holding because ebits are specific private bits). Exact definitions and more details are given in Supplementary Note 1.

To state our upper bound for $\mathcal{C}(\{\mathcal{E}_i\})$, we introduce the notion of channel simulation, as generally formulated by ref. [15] (see also refs. [32–37] for variants). Recall that any quantum channel $\mathcal{E}$ is simulable by applying a trace-preserving LOCC $\mathcal{T}$ to the input state ρ together with some bipartite resource state σ, so that $\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \sigma)$. The pair $(\mathcal{T}, \sigma)$ represents a possible "LOCC simulation" of the channel. In particular, for channels that suitably commute with the random unitaries of teleportation[4], called "teleportation-covariant" channels[15], one finds that $\mathcal{T}$ is teleportation and σ is their Choi matrix $\sigma_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi)$, where Φ is a maximally entangled state. The latter is also known as "teleportation simulation".

For bosonic channels, the Choi matrices are energy-unbounded, so that simulations need to be formulated asymptotically. In general, an asymptotic state σ is defined as the limit of a sequence of physical states σ^μ, i.e., $\sigma := \lim_\mu \sigma^\mu$. The simulation of a channel $\mathcal{E}$ over an asymptotic state takes the form $\|\mathcal{E}(\rho) - \mathcal{T}(\rho \otimes \sigma^\mu)\|_1 \xrightarrow{\mu} 0$ where the LOCC $\mathcal{T}$ may also depend

on μ in the general case[15]. Similarly, any relevant functional on the asymptotic state needs to be computed over the defining sequence σ^μ before taking the limit for large μ. These technicalities are fully accounted in the Methods section.

The other notion to introduce is that of entanglement cut between Alice and Bob. In the setting of a linear chain, a cut "i" disconnects channel $\mathcal{E}_i$ between repeaters $\mathbf{r}_i$ and $\mathbf{r}_{i+1}$. Such channel can be replaced by a simulation with some resource state σ_i. After calculations (see Methods), this allows us to write

$$\mathcal{C}(\{\mathcal{E}_i\}) \leq E_{\mathrm{R}}(\sigma_i), \tag{1}$$

where $E_{\mathrm{R}}(\cdot)$ is the relative entropy of entanglement (REE). Recall that the REE is defined as[38–40]

$$E_{\mathrm{R}}(\sigma) = \inf_{\gamma\in\mathrm{SEP}} S(\sigma||\gamma), \tag{2}$$

where SEP represents the ensemble of separable bipartite states and $S(\sigma||\gamma) := \mathrm{Tr}\left[\sigma(\log_2\sigma - \log_2\gamma)\right]$ is the relative entropy. In general, for any asymptotic state defined by the limit $\sigma := \lim_\mu \sigma^\mu$, we may extend the previous definition and consider

$$E_{\mathrm{R}}(\sigma) = \liminf_\mu E_{\mathrm{R}}(\sigma^\mu) = \inf_{\gamma^\mu} \liminf_\mu S(\sigma^\mu||\gamma^\mu), \tag{3}$$

where γ^μ is a converging sequence of separable states[15].

By minimizing Eq. (1) over all cuts, we may write

$$\mathcal{C}(\{\mathcal{E}_i\}) \leq \min_i E_{\mathrm{R}}(\sigma_i), \tag{4}$$

which establishes the ultimate limit for entanglement and key distribution through a repeater chain. For a chain of teleportation-covariant channels, we may use their teleportation simulation over Choi matrices and write

$$\mathcal{C}(\{\mathcal{E}_i\}) \leq \min_i E_{\mathrm{R}}(\sigma_{\mathcal{E}_i}). \tag{5}$$

Note that the family of teleportation-covariant channels is large, including Pauli channels (at any dimension)[7] and bosonic Gaussian channels[9]. Within such a family, there are channels $\mathcal{E}$ whose generic two-way capacity $\mathcal{C} = Q_2$, D_2 or K satisfies

$$\mathcal{C}(\mathcal{E}) = E_{\mathrm{R}}(\sigma_{\mathcal{E}}) = D_1(\sigma_{\mathcal{E}}), \tag{6}$$

where $D_1(\sigma_{\mathcal{E}})$ is the one-way distillable entanglement of the Choi matrix (defined as an asymptotic functional in the bosonic case[15]). These are called "distillable channels" and include bosonic lossy channels, quantum-limited amplifiers, dephasing and erasure channels[15].

For a chain of distillable channels, we therefore exactly establish the repeater-assisted capacity as

$$\mathcal{C}(\{\mathcal{E}_i\}) = \min_i \mathcal{C}(\mathcal{E}_i) = \min_i E_{\mathrm{R}}(\sigma_{\mathcal{E}_i}). \tag{7}$$

In fact the upper bound ($\leq$) follows from Eqs. (5) and (6). The lower bound ($\geq$) relies on the fact that an achievable rate for end-to-end entanglement distribution consists in: (i) each pair, $\mathbf{r}_i$ and $\mathbf{r}_{i+1}$, exchanging $D_1(\sigma_{\mathcal{E}_i})$ ebits over $\mathcal{E}_i$; and (ii) performing entanglement swapping on the distilled ebits. In this way, at least $\min_i D_1(\sigma_{\mathcal{E}_i})$ ebits are shared between Alice and Bob.

Lossy chains. Let us specify Eq. (7) to an important case. For a chain of quantum repeaters connected by lossy channels with transmissivities $\{\eta_i\}$, we find the capacity

$$\mathcal{C}_{\mathrm{loss}} = -\log_2(1-\eta_{\mathrm{min}}), \quad \eta_{\mathrm{min}} := \min_i \eta_i. \tag{8}$$

Thus, the minimum transmissivity within the lossy chain establishes the ultimate rate for repeater-assisted quantum/private communication between the end-users. For instance, consider an optical fiber with transmissivity η and insert N repeaters so that the fiber is split into $N+1$ lossy channels. The optimal configuration corresponds to equidistant repeaters, so that $\eta_{\mathrm{min}} = \sqrt[N+1]{\eta}$ and the maximum capacity of the lossy chain is

$$\mathcal{C}_{\mathrm{loss}}(\eta, N) = -\log_2\left(1 - \sqrt[N+1]{\eta}\right). \tag{9}$$

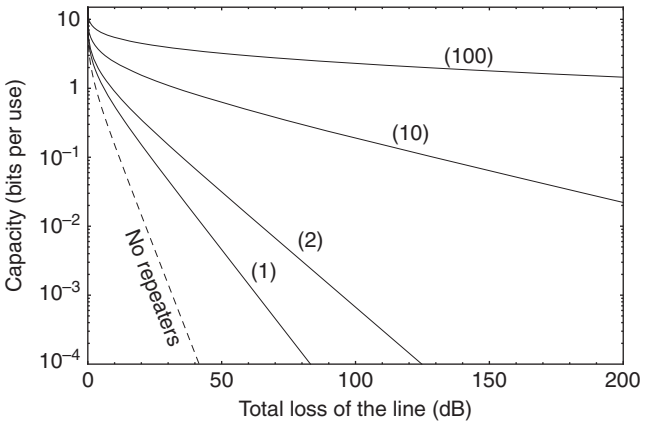

Fig. 2 Optimal performance of lossy chains. Capacity (target bits per chain use) versus total loss of the line (decibels, dB) for $N = 1, 2, 10$ and 100 equidistant repeaters. Compare the repeater-assisted capacities (solid curves) with the point-to-point repeater-less bound[15] (dashed curve)

This capacity is plotted in Fig. 2 and compared with the point-to-point PLOB bound $\mathcal{C}(\eta) = \mathcal{C}_{\mathrm{loss}}(\eta, 0)$. A simple calculation shows that if we want to guarantee a performance of 1 target bit per use of the chain, then we may tolerate at most 3 dB of loss in each individual link. This "3dB rule" imposes a maximum repeater-repeater distance of 15 km in standard optical fiber (at 0.2dB/km).

Quantum networks under single-path routing. A quantum communication network can be represented by an undirected finite graph[18] $\mathcal{N} = (P, E)$, where P is the set of points and E the set of all edges. Each point $\mathbf{p}$ has a local register of quantum systems. Two points $\mathbf{p}_i$ and $\mathbf{p}_j$ are connected by an edge $(\mathbf{p}_i, \mathbf{p}_j) \in E$ if there is a quantum channel $\mathcal{E}_{ij} := \mathcal{E}_{\mathbf{p}_i\mathbf{p}_j}$ between them. By simulating each channel $\mathcal{E}_{ij}$ with a resource state σ_{ij}, we simulate the entire network $\mathcal{N}$ with a set of resource states $\sigma(\mathcal{N}) = \{\sigma_{ij}\}$. A route is an undirected path $\mathbf{a} - \mathbf{p}_i - \cdots - \mathbf{p}_j - \mathbf{b}$ between the two end-points, Alice $\mathbf{a}$ and Bob $\mathbf{b}$. These are connected by an ensemble of possible routes $\Omega = \{1, \ldots, \omega, \ldots\}$, with the generic route ω involving the transmission through a sequence of channels $\{\mathcal{E}_0^\omega, \ldots, \mathcal{E}_k^\omega \ldots\}$. Finally, an entanglement cut C is a bipartition $(\mathbf{A}, \mathbf{B})$ of P such that $\mathbf{a} \in \mathbf{A}$ and $\mathbf{b} \in \mathbf{B}$. Any such cut C identifies a super Alice $\mathbf{A}$ and a super Bob $\mathbf{B}$, which are connected by the cut-set $\tilde{C} = \{(\mathbf{x}, \mathbf{y}) \in E : \mathbf{x} \in \mathbf{A}, \mathbf{y} \in \mathbf{B}\}$. See the example in Fig. 3 and more details in Supplementary Notes 2 and 3.

Let us remark that the quantum network is here described by an undirected graph where the physical direction of the quantum channels $\mathcal{E}_{ij}$ can be forward ($\mathbf{p}_i \to \mathbf{p}_j$) or backward ($\mathbf{p}_j \to \mathbf{p}_i$). As said before for the repeater chains, this degree of freedom relies on the fact that we consider assistance by two-way CC, so that the optimal transmission of qubits can always be reduced to the distillation of ebits followed by teleportation. The logical flow of quantum information is therefore fully determined by the LOs of the points, not by the physical direction of the quantum channel which is used to exchange a quantum system along an edge of the network. This study of an undirected quantum network under two-way CC clearly departs from other investigations[41–43].

In a sequential protocol $\mathcal{P}_{\mathrm{seq}}$, the network is initialized by a preliminary network LOCC, where all the points communicate

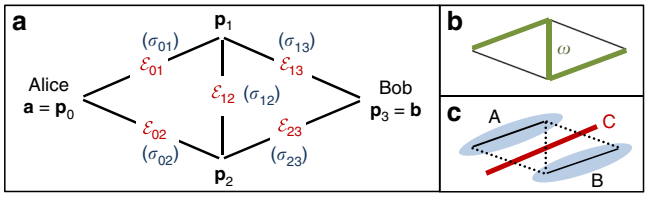

Fig. 3 Diamond quantum network $\mathcal{N}^{\diamondsuit}$. **a** This is a quantum network of four points $P = \{\mathbf{p}_0, \mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3\}$, with end-points $\mathbf{p}_0 = \mathbf{a}$ (Alice) and $\mathbf{p}_3 = \mathbf{b}$ (Bob). Two points $\mathbf{p}_i$ and $\mathbf{p}_j$ are connected by an edge $(\mathbf{p}_i, \mathbf{p}_j)$ if there is an associated quantum channel $\mathcal{E}_{ij}$. This channel has a corresponding resource state σ_{ij} in a simulation of the network. There are four (simple) routes: $1 : \mathbf{a} - \mathbf{p}_1 - \mathbf{b}$, $2 : \mathbf{a} - \mathbf{p}_2 - \mathbf{b}$, $3 : \mathbf{a} - \mathbf{p}_2 - \mathbf{p}_1 - \mathbf{b}$, and $4 : \mathbf{a} - \mathbf{p}_1 - \mathbf{p}_2 - \mathbf{b}$. As an example, route 4 involves the transmission through the sequence of quantum channels $\{\mathcal{E}_k^4\}$ which is defined by $\mathcal{E}_0^4 := \mathcal{E}_{01}$, $\mathcal{E}_1^4 := \mathcal{E}_{12}$ and $\mathcal{E}_2^4 := \mathcal{E}_{23}$. **b** We explicitly show route $\omega = 4$. In a sequential protocol, each use of the network corresponds to using a single route ω between the two end-points, with some probability p_ω. **c** We show an entanglement cut C of the network, with super Alice **A** and super Bob **B** made by the points in the two clouds. These are connected by the cut-set $\tilde{C}$ composed by the dotted edges

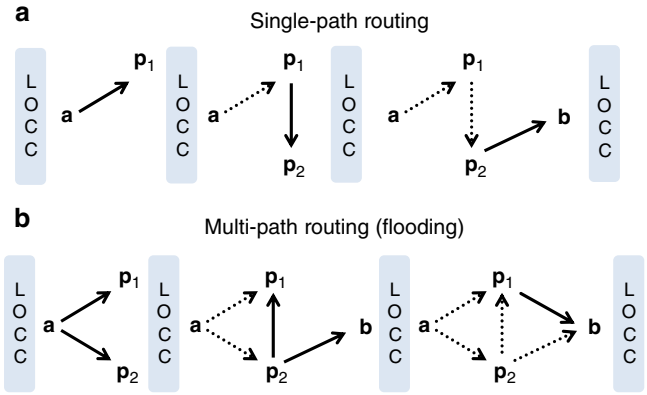

Fig. 4 Network protocols of quantum and private communication. **a** In a sequential protocol, systems are routed through a single path probabilistically chosen by the points. Here it is $\mathbf{a} - \mathbf{p}_1 - \mathbf{p}_2 - \mathbf{b}$. Each transmission occurs between two adaptive LOCCs, where all points of the network perform LOs assisted by two-way CC. **b** In a flooding protocol, systems are simultaneously routed from Alice to Bob through a sequence of multipoint communications in such a way that each edge of the network is used exactly once in an end-to-end transmission. Here we show a possible sequence $\mathbf{a} \to \{\mathbf{p}_1, \mathbf{p}_2\}$, $\mathbf{p}_2 \to \{\mathbf{p}_1, \mathbf{b}\}$, $\mathbf{p}_1 \to \{\mathbf{b}\}$. Each multipoint communication occurs between two adaptive LOCCs

with each other via unlimited two-way CCs and perform adaptive LOs on their local quantum systems. With some probability, Alice exchanges a quantum system with repeater $\mathbf{p}_i$, followed by a second network LOCC; then repeater $\mathbf{p}_i$ exchanges a system with repeater $\mathbf{p}_j$, followed by a third network LOCC and so on, until Bob is reached through some route in a complete sequential use of the network (see Fig. 4). The routing is itself adaptive in the general case, with each node updating its routing table (probability distribution) on the basis of the feedback received by the other nodes. For large n uses of the network, there is a probability distribution associated with the ensemble Ω, with the generic route ω being used np_ω times. Alice and Bob's output state $\rho_{\mathbf{ab}}^n$ will approximate a target state with nR_n bits. By optimizing over $\mathcal{P}_{\text{seq}}$ and taking the limit of large n, we define the sequential or single-path capacity of the network $\mathcal{C}(\mathcal{N})$, whose nature depends on the target bits.

To state our upper bound, let us first introduce the flow of REE through a cut. Given an entanglement cut C of the network, consider its cut-set $\tilde{C}$. For each edge $(\mathbf{x}, \mathbf{y})$ in $\tilde{C}$, we have a channel $\mathcal{E}_{\mathbf{xy}}$ and a corresponding resource state $\sigma_{\mathbf{xy}}$ associated with a simulation. Then we define the single-edge flow of REE across cut C as

$$E_{\text{R}}(C) := \max_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\text{R}}(\sigma_{\mathbf{xy}}). \tag{10}$$

The minimization of this quantity over all entanglement cuts provides our upper bound for the single-path capacity of the network, i.e.,

$$\mathcal{C}(\mathcal{N}) \leq \min_{C} E_{\text{R}}(C), \tag{11}$$

which is the network generalization of Eq. (4). For proof see Methods and further details in Supplementary Note 4.

In Eq. (11), the quantity $E_{\text{R}}(C)$ represents the maximum entanglement (as quantified by the REE) "flowing" through a cut. Its minimization over all the cuts bounds the single-path capacity for quantum communication, entanglement distribution and key generation. For a network of teleportation-covariant channels, the resource state $\sigma_{\mathbf{xy}}$ in Eq. (10) is the Choi matrix $\sigma_{\mathcal{E}_{\mathbf{xy}}}$ of the channel $\mathcal{E}_{\mathbf{xy}}$. In particular, for a network of distillable channels, we may also set

$$\mathcal{C}(\mathcal{E}_{\mathbf{xy}}) = E_{\text{R}}(\sigma_{\mathcal{E}_{\mathbf{xy}}}) = D_1(\sigma_{\mathcal{E}_{\mathbf{xy}}}), \tag{12}$$

for any edge $(\mathbf{x}, \mathbf{y})$. Therefore, we may refine the previous bound of Eq. (11) into $\mathcal{C}(\mathcal{N}) \leq \min_C \mathcal{C}(C)$ where

$$\mathcal{C}(C) := \max_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \mathcal{C}(\mathcal{E}_{\mathbf{xy}}) \tag{13}$$

is the maximum (single-edge) capacity of a cut.

Let us now derive a lower bound. First we prove that, for an arbitrary network, $\min_C \mathcal{C}(C) = \max_\omega \mathcal{C}(\omega)$, where $\mathcal{C}(\omega) := \min_i \mathcal{C}(\mathcal{E}_i^\omega)$ is the capacity of route ω (see Methods and Supplementary Note 4 for more details). Then, we observe that $\mathcal{C}(\omega)$ is an achievable rate. In fact, any two consecutive points on route ω may first communicate at the rate $\mathcal{C}(\mathcal{E}_i^\omega)$; the distributed resources are then swapped to the end-users, e.g., via entanglement swapping or key composition at the minimum rate $\min_i \mathcal{C}(\mathcal{E}_i^\omega)$. For a distillable network, this lower bound coincides with the upper bound, so that we exactly establish the single-path capacity as

$$\mathcal{C}(\mathcal{N}) = \max_{\omega} \mathcal{C}(\omega) = \min_{C} \mathcal{C}(C) = \min_{C} E_{\text{R}}(C). \tag{14}$$

Finding the optimal route ω_* corresponds to solving the widest path problem[24] where the weights of the edges $(\mathbf{x}, \mathbf{y})$ are the two-way capacities $\mathcal{C}(\mathcal{E}_{\mathbf{xy}})$. Route ω_* can be found via modified Dijkstra's shortest path algorithm[25], working in time $O(|E| \log_2 |P|)$, where $|E|$ is the number of edges and $|P|$ is the number of points. Over route ω_* a capacity-achieving protocol is non adaptive, with point-to-point sessions of one-way entanglement distillation followed by entanglement swapping[4]. In a practical implementation, the number of distilled ebits can be computed using the methods from ref. [44]. Also note that, because the swapping is on ebits, there is no violation of the Bellman's optimality principle[45].

An important example is an optical lossy network $\mathcal{N}_{\text{loss}}$ where any route ω is composed of lossy channels with transmissivities $\{\eta_i^\omega\}$. Denote by $\eta_\omega := \min_i \eta_i^\omega$ the end-to-end transmissivity of route ω. The single-path capacity is given by the route with maximum transmissivity

$$\mathcal{C}(\mathcal{N}_{\text{loss}}) = -\log_2(1 - \eta_{\mathcal{N}}), \quad \eta_{\mathcal{N}} := \max_{\omega\in\Omega} \eta_\omega. \tag{15}$$

In particular, this is the ultimate rate at which the two end-points may generate secret bits per sequential use of the lossy network.

Quantum networks under multi-path routing. In a network we may consider a more powerful routing strategy, where systems are transmitted through a sequence of multipoint communications (interleaved by network LOCCs). In each of these communications, a number M of quantum systems are prepared in a generally multipartite state and simultaneously transmitted to M receiving nodes. For instance, as shown in the example of Fig. 4, Alice may simultaneously sends systems to repeaters $\mathbf{p}_1$ and $\mathbf{p}_2$, which is denoted by $\mathbf{a} \to \{\mathbf{p}_1, \mathbf{p}_2\}$. Then, repeater $\mathbf{p}_2$ may communicate with repeater $\mathbf{p}_1$ and Bob $\mathbf{b}$, i.e., $\mathbf{p}_2 \to \{\mathbf{p}_1, \mathbf{b}\}$. Finally, repeater $\mathbf{p}_1$ may communicate with Bob, i.e., $\mathbf{p}_1 \to \mathbf{b}$. Note that each edge of the network is used exactly once during the end-to-end transmission, a strategy known as "flooding" in computer networks[46]. This is achieved by non-overlapping multipoint communications, where the receiving repeaters choose unused edges for the next transmissions. More generally, each multipoint communication is assumed to be a point-to-multipoint connection with a logical sender-to-receiver(s) orientation but where the quantum systems may be physically transmitted either forward or backward by the quantum channels.

Thus, in a general quantum flooding protocol $\mathcal{P}_{\text{flood}}$, the network is initialized by a preliminary network LOCC. Then, Alice $\mathbf{a}$ exchanges quantum systems with all her neighbor repeaters $\mathbf{a} \to \{\mathbf{p}_k\}$. This is followed by another network LOCC. Then, each receiving repeater exchanges systems with its neighbor repeaters through unused edges, and so on. Each multipoint communication is interleaved by network LOCCs and may distribute multi-partite entanglement. Eventually, Bob is reached as an end-point in the first parallel use of the network, which is completed when all Bob's incoming edges have been used exactly once. In the limit of many uses n and optimizing over $\mathcal{P}_{\text{flood}}$, we define the multi-path capacity of the network $\mathcal{C}^{\text{m}}(\mathcal{N})$.

As before, given an entanglement cut C, consider its cut-set $\tilde{C}$. For each edge $(\mathbf{x}, \mathbf{y})$ in $\tilde{C}$, there is a channel $\mathcal{E}_{\mathbf{xy}}$ with a corresponding resource state $\sigma_{\mathbf{xy}}$. We define the multi-edge flow of REE through C as

$$E_{\text{R}}^{\text{m}}(C) := \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\text{R}}(\sigma_{\mathbf{xy}}), \tag{16}$$

which is the total entanglement (REE) flowing through a cut. The minimization of this quantity over all entanglement cuts provides our upper bound for the multi-path capacity of the network, i.e.,

$$\mathcal{C}^{\text{m}}(\mathcal{N}) \leq \min_{C} E_{\text{R}}^{\text{m}}(C), \tag{17}$$

which is the multi-path generalization of Eq. (11). For proof see Methods and further details in Supplementary Note 5. In a teleportation-covariant network we may simply use the Choi matrices $\sigma_{\mathbf{xy}} = \sigma_{\mathcal{E}_{\mathbf{xy}}}$. Then, for a distillable network, we may use $E_{\text{R}}(\sigma_{\mathcal{E}_{\mathbf{xy}}}) = \mathcal{C}(\mathcal{E}_{\mathbf{xy}})$ from Eq. (12), and write the refined upper bound $\mathcal{C}^{\text{m}}(\mathcal{N}) \leq \min_C \mathcal{C}^{\text{m}}(C)$, where

$$\mathcal{C}^{\text{m}}(C) := \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \mathcal{C}(\mathcal{E}_{\mathbf{xy}}) \tag{18}$$

is the total (multi-edge) capacity of a cut.

To show that the upper bound is achievable for a distillable network, we need to determine the optimal flow of qubits from Alice to Bob. First of all, from the knowledge of the capacities $\mathcal{C}(\mathcal{E}_{\mathbf{xy}})$, the parties solve a classical problem of maximum flow[26–29] compatible with those capacities. By using Orlin's algorithm[47], the solution can be found in $O(|P|\times|E|)$ time. This provides an optimal orientation for the network and the rates $R_{\mathbf{xy}} \leq \mathcal{C}(\mathcal{E}_{\mathbf{xy}})$ to be used. Then, any pair of neighbor points, $\mathbf{x}$ and $\mathbf{y}$, distill $nR_{\mathbf{xy}}$ ebits via one-way CCs. Such ebits are used to teleport $nR_{\mathbf{xy}}$ qubits from $\mathbf{x}$ to $\mathbf{y}$ according to the optimal orientation. In this way, a number nR of qubits are teleported from Alice to Bob, flowing as quantum information through the network. Using the max-flow min-cut theorem[26–29,47–53], we have that the maximum flow is $n\mathcal{C}^{\text{m}}(C_{\min})$ where $C_{\min}$ is the minimum cut, i.e., $\mathcal{C}^{\text{m}}(C_{\min}) = \min_C \mathcal{C}^{\text{m}}(C)$. Thus, that for a distillable $\mathcal{N}$, we find the multi-path capacity

$$\mathcal{C}^{\text{m}}(\mathcal{N}) = \min_{C} \mathcal{C}^{\text{m}}(C) = \min_{C} E_{\text{R}}^{\text{m}}(C), \tag{19}$$

which is the multi-path version of Eq. (14). This is achievable by using a non adaptive protocol where the optimal routing is given by Orlin's algorithm[47].

As an example, consider again a lossy optical network $\mathcal{N}_{\text{loss}}$ whose generic edge $(\mathbf{x}, \mathbf{y})$ has transmissivity $\eta_{\mathbf{xy}}$. Given a cut C, consider its loss $L_C := \prod_{(\mathbf{x},\mathbf{y})\in\tilde{C}}(1-\eta_{\mathbf{xy}})$ and define the total loss of the network as the maximization $L_{\mathcal{N}} := \max_C L_C$. We find that the multi-path capacity is just given by

$$\mathcal{C}^{\text{m}}(\mathcal{N}_{\text{loss}}) = -\log_2 L_{\mathcal{N}}. \tag{20}$$

It is interesting to make a direct comparison between the performance of single- and multi-path strategies. For this purpose, consider a diamond network $\mathcal{N}_{\text{loss}}^{\diamondsuit}$ whose links are lossy channels with the same transmissivity η. In this case, we easily see that the multi-path capacity doubles the single-path capacity of the network, i.e.,

$$\mathcal{C}^{\text{m}}(\mathcal{N}_{\text{loss}}^{\diamondsuit}) = 2\mathcal{C}(\mathcal{N}_{\text{loss}}^{\diamondsuit}) = -2\log_2(1-\eta). \tag{21}$$

As expected the parallel use of the quantum network is more powerful than the sequential use.

Formulas for distillable chains and networks. Here we provide explicit analytical formulas for the end-to-end capacities of distillable chains and networks, beyond the lossy case already studied above. In fact, examples of distillable channels are not only lossy channels but also quantum-limited amplifiers, dephasing and erasure channels. First let us recall their explicit definitions and their two-way capacities.

A lossy (pure-loss) channel with transmissivity $\eta \in (0,1)$ corresponds to a specific phase-insensitive Gaussian channel which transforms input quadratures $\hat{\mathbf{x}} = (\hat{q}, \hat{p})^T$ as $\hat{\mathbf{x}} \to \sqrt{\eta}\hat{\mathbf{x}} + \sqrt{1-\eta}\hat{\mathbf{x}}_E$, where E is the environment in the vacuum state[9]. Its two-way capacities (Q_2, D_2 and K) all coincide and are given by the PLOB bound[15]

$$\mathcal{C}(\eta) = -\log_2(1-\eta). \tag{22}$$

A quantum-limited amplifier with an associated gain $g > 1$ is another phase-insensitive Gaussian channel but realizing the transformation $\hat{\mathbf{x}} \to \sqrt{g}\hat{\mathbf{x}} + \sqrt{g-1}\hat{\mathbf{x}}_E$, where the environment E is in the vacuum state[9]. Its two-way capacities all coincide and are given by[15]

$$\mathcal{C}(g) = -\log_2(1-g^{-1}). \tag{23}$$

A dephasing channel with probability $p \leq 1/2$ is a Pauli channel of the form $\rho \to (1-p)\rho + pZ\rho Z$, where Z is the phase-flip Pauli operator[7]. Its two-way capacities all coincide and are given by[15]

$$\mathcal{C}(p) = 1 - H_2(p), \tag{24}$$

where $H_2(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary Shannon entropy. Finally, an erasure channel with probability $p \leq 1/2$ is a channel of the form $\rho \to (1-p)\rho + p|e\rangle\langle e|$, where $|e\rangle\langle e|$ is an orthogonal state living in an extra dimension[7]. Its two-

Table 1 Analytical formulas for the end-to-end capacities of distillable chains and networks

	Chain $\{\mathcal{E}_i\}$ – Repeater capacity $\mathcal{C}(\{\mathcal{E}_i\})$	**Network $\mathcal{N}$ – Single-path capacity** $\mathcal{C}(\mathcal{N})$	**Network $\mathcal{N}$ – Multi-path capacity** $\mathcal{C}^m(\mathcal{N})$
Lossy channels (transmissivity η)	$-\log_2(1-\min_i \eta_i)$	$-\log_2(1-\eta_{\mathcal{N}})$	$-\log_2 L_{\mathcal{N}}$
Q-limited amplifiers (gain g)	$-\log_2\left[1-(\max_i g_i)^{-1}\right]$	$-\log_2(1-g_{\mathcal{N}}^{-1})$	$-\log_2 G_{\mathcal{N}}$
Dephasing channels (probability p)	$1-H_2(\max_i p_i)$	$1-H_2(p_{\mathcal{N}})$	$\min_C \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}\left[1-H_2(p_{\mathbf{xy}})\right]$
Erasure channels (probability p)	$1-\max_i p_i$	$1-p_{\mathcal{N}}$	$\min_C \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}(1-p_{\mathbf{xy}})$

way capacities all coincide to[15,54,55]

$$\mathcal{C}(p)=1-p. \tag{25}$$

Consider now a repeater chain $\{\mathcal{E}_i\}$, where the channels $\mathcal{E}_i$ are distillable of the same type (e.g., all quantum-limited amplifiers with different gains g_i). The repeater-assisted capacity can be computed by combining Eq. (7) with one of the Eqs. (22)–(25). The final formulas are shown in the first column of Table 1. Then consider a quantum network $\mathcal{N}=(P,E)$, where each edge $(\mathbf{x},\mathbf{y})\in E$ is described by a distillable channel $\mathcal{E}_{\mathbf{xy}}$ of the same type. For network $\mathcal{N}$, we may consider both a generic route $\omega\in\Omega$, with sequence of channels $\mathcal{E}_i^{\omega}$, and a entanglement cut C, with corresponding cut-set $\tilde{C}$. By combining Eqs. (14) and (19) with Eqs. (22)–(25), we derive explicit formulas for the single-path and multi-path capacities. These are given in the second and third columns of Table 1 where we set

$$\eta_{\mathcal{N}}:=\max_{\omega\in\Omega}\min_i \eta_i^{\omega}=\min_C \max_{(\mathbf{x},\mathbf{y})\in\tilde{C}}\eta_{\mathbf{xy}}, \tag{26}$$

$$g_{\mathcal{N}}:=\min_{\omega\in\Omega}\max_i g_i^{\omega}=\max_C \min_{(\mathbf{x},\mathbf{y})\in\tilde{C}} g_{\mathbf{xy}}, \tag{27}$$

$$p_{\mathcal{N}}:=\min_{\omega\in\Omega}\max_i p_i^{\omega}=\max_C \min_{(\mathbf{x},\mathbf{y})\in\tilde{C}} p_{\mathbf{xy}}, \tag{28}$$

$$L_{\mathcal{N}}:=\max_C \prod_{(\mathbf{x},\mathbf{y})\in\tilde{C}}(1-\eta_{\mathbf{xy}}), \tag{29}$$

$$G_{\mathcal{N}}:=\max_C \prod_{(\mathbf{x},\mathbf{y})\in\tilde{C}}(1-g_{\mathbf{xy}}^{-1}). \tag{30}$$

Let us note that the formulas for dephasing and erasure channels can be easily extended to arbitrary dimension d. In fact, a qudit erasure channel is formally defined as before and its two-way capacities are[15,54,55]

$$\mathcal{C}(p)=(1-p)\log_2 d. \tag{31}$$

Therefore, it is sufficient to multiply by $\log_2 d$ the corresponding expressions in Table 1. Then, in arbitrary dimension d, the dephasing channel is defined as

$$\rho\to\sum_{k=0}^{d-1} p_k Z_d^k \rho (Z_d^{\dagger})^k, \tag{32}$$

where p_k is the probability of k phase flips and $Z_d^k|i\rangle=\exp(2\pi i k d^{-1})|i\rangle$. Its generic two-way capacity is[15]

$$\mathcal{C}(p,d)=\log_2 d-H(\{p_k\}), \tag{33}$$

where $H(\{p_k\}):=-\sum_k p_k\log_2 p_k$ is the Shannon entropy. Here the generalization is also simple. For instance, in a chain $\{\mathcal{E}_i\}$ of such d-dimensional dephasing channels, we would have $N+1$ distributions $\{p_k^i\}$. We then compute the most entropic distribution, i.e., we take the maximization $\max_i H(\{p_k^i\})$. This is the bottleneck that determines the repeater capacity, so that

$$\mathcal{C}(\{p_k^i\})=\log_2 d-\max_i H(\{p_k^i\}). \tag{34}$$

Generalization to dimension d is also immediate for the two network capacities $\mathcal{C}$ and $\mathcal{C}^{\mathrm{m}}$.

Discussion

This work establishes the ultimate boundaries of quantum and private communications assisted by repeaters, from the case of a single repeater chain to an arbitrary quantum network under single- or multi-path routing. Assuming arbitrary quantum channels between the nodes, we have shown that the end-to-end capacities are bounded by single-letter quantities based on the relative entropy of entanglement. These upper bounds are very general and also apply to chains and networks with untrusted nodes (i.e., run by an eavesdropper). Our theory is formulated in a general information-theoretic fashion which also applies to other entanglement measures, as discussed in our Methods section. The upper bounds are particularly important because they set the tightest upper limits on the performance of quantum repeaters in various network configurations. For instance, our benchmarks may be used to evaluate performances in relay-assisted QKD protocols such as MDI-QKD and variants[56–58]. Related literature and other developments[59–66] are discussed in Supplementary Note 6.

For the lower bounds, we have employed classical composition methods of the capacities, either based on the widest path problem or the maximum flow, depending on the type of routing. In general, these simple and classical lower bounds do not coincide with the quantum upper bounds. However this is remarkably the case for distillable networks, for which the ultimate quantum communication performance can be completely reduced to the resolution of classical problems of network information theory. For these networks, widest path and maximum flow determine the quantum performance in terms of secret key generation, entanglement distribution and transmission of quantum information. In this way, we have been able to exactly establish the various end-to-end capacities of distillable chains and networks where the quantum systems are affected by the most fundamental

noise models, including bosonic loss, which is the most important for optical and telecom communications, quantum-limited amplification, dephasing and erasure. In particular, our results also showed how the parallel or "broadband" use of a lossy quantum network via multi-path routing may greatly improve the end-to-end rates.

Methods

We present the main techniques that are needed to prove the results of our main text. These methods are here provided for a more general entanglement measure $E_{\rm M}$, and specifically apply to the REE. We consider a quantum network $\mathcal{N}$ under single- or multi-path routing. In particular, a chain of quantum repeaters can be treated as a single-route quantum network.

For the upper bounds, our methodology can be broken down in the following steps: (i) Derivation of a general weak converse upper bound in terms of a suitable entanglement measure (in particular, the REE); (ii) Simulation of the quantum network, so that quantum channels are replaced by resource states; (iii) Stretching of the network with respect to an entanglement cut, so that Alice and Bob's shared state has a simple decomposition in terms of resource states; (iv) Data processing, subadditivity over tensor-products, and minimization over entanglement cuts. These steps provide entanglement-based upper bounds for the end-to-end capacities. For the lower bounds, we perform a suitable composition of the point-to-point capacities of the single-link channels by means of the widest path and the maximum flow, depending on the routing. For the case of distillable quantum networks (and chains), these lower bounds coincide with the upper bounds expressed in terms of the REE.

General (weak converse) upper bound. This closely follows the derivation of the corresponding point-to-point upper bound first given in the second 2015 arXiv version of ref. [15] and later reported as Theorem 2 in ref. [16]. Consider an arbitrary end-to-end $(n, R_n^\varepsilon, \varepsilon)$ network protocol $\mathcal{P}$ (single- or multi-path). This outputs a shared state $\rho_{\mathbf{ab}}^n$ for Alice and Bob after n uses, which is ε-close to a target private state[30,31] ϕ^n having nR_n^ε secret bits, i.e., in trace norm we have $\left\|\rho_{\mathbf{ab}}^n - \phi^n\right\|_1 \leq \varepsilon$. Consider now an entanglement measure $E_{\rm M}$ which is normalized on the target state, i.e.,

$$E_{\rm M}(\phi^n) \geq nR_n^\varepsilon. \tag{35}$$

Assume that $E_{\rm M}$ is continuous. This means that, for d-dimensional states ρ and σ that are close in trace norm as $\|\rho - \sigma\|_1 \leq \varepsilon$, we may write

$$|E_{\rm M}(\rho) - E_{\rm M}(\sigma)| \leq g(\varepsilon)\log_2 d + h(\varepsilon), \tag{36}$$

with the functions g and h converging to zero in ε. Assume also that E_M is monotonic under trace-preserving LOCCs $\bar{\Lambda}$, so that

$$E_{\rm M}[\bar{\Lambda}(\rho)] \leq E_{\rm M}(\rho), \tag{37}$$

a property which is also known as data processing inequality. Finally, assume that $E_{\rm M}$ is subadditive over tensor products, i.e.,

$$E_{\rm M}(\rho^{\otimes n}) \leq nE_{\rm M}(\rho). \tag{38}$$

All these properties are certainly satisfied by the REE $E_{\rm R}$ and the squashed entanglement (SQ) $E_{\rm SQ}$, with specific expressions for g and h (e.g., these expressions are explicitly reported in Sec. VIII.A of ref. [16]).

Using the first two properties (normalization and continuity), we may write

$$R_n^\varepsilon \leq \frac{E_{\rm M}(\rho_{\mathbf{ab}}^n) + g(\varepsilon)\log_2 d + h(\varepsilon)}{n}, \tag{39}$$

where d is the dimension of the target private state. We know that this dimension is at most exponential in the number of uses, i.e., $\log_2 d \leq \alpha n R_n^\varepsilon$ for constant α (e.g., see ref. [15] or Lemma 1 in ref. [16]). By replacing this dimensional bound in Eq. (39), taking the limit for large n and small ε (weak converse), we derive

$$\lim_\varepsilon \lim_n R_n^\varepsilon \leq \lim_n \frac{E_{\rm M}(\rho_{\mathbf{ab}}^n)}{n}. \tag{40}$$

Finally, we take the supremum over all protocols $\mathcal{P}$ so that we can write our general upper bound for the end-to-end secret key capacity (SKC) of the network

$$E_{\rm M}^*(\mathcal{N}) := \sup_{\mathcal{P}} \lim_n \frac{E_{\rm M}(\rho_{\mathbf{ab}}^n)}{n}. \tag{41}$$

In particular, this is an upper bound to the single-path SKC $\mathcal{K}$ if $\mathcal{P}$ are single-path protocols, and to the multi-path SKC $\mathcal{K}^m$ if $\mathcal{P}$ are multi-path (flooding) protocols.

In the case of an infinite-dimensional state $\rho_{\mathbf{ab}}^n$, the proof can be repeated by introducing a truncation trace-preserving LOCC $\boldsymbol{T}$, so that $\delta_{\mathbf{ab}}^n = \boldsymbol{T}(\rho_{\mathbf{ab}}^n)$ is a finite-dimensional state. The proof is repeated for $\delta_{\mathbf{ab}}^n$ and finally we use the data processing $E_{\rm M}(\delta_{\mathbf{ab}}^n) \leq E_{\rm M}(\rho_{\mathbf{ab}}^n)$ to write the same upper bound as in Eq. (41). This follows the same steps of the proof given in the second 2015 arXiv version of ref. [15] and later reported as Theorem 2 in ref. [16]. It is worth mentioning that Eq. (41) can equivalently be proven without using the exponential growth of the private state, i.e., using the steps of the third proof given in the Supplementary Note 3 of ref. [15].

Network simulation. Given a network $\mathcal{N} = (P, E)$ with generic point $\mathbf{x} \in P$ and edge $(\mathbf{x}, \mathbf{y}) \in E$, replace the generic channel $\mathcal{E}_{\mathbf{xy}}$ with a simulation over a resource state $\sigma_{\mathbf{xy}}$. This means to write $\mathcal{E}_{\mathbf{xy}}(\rho) = \mathcal{T}_{\mathbf{xy}}(\rho \otimes \sigma_{\mathbf{xy}})$ for any input state ρ, by resorting to a suitable trace-preserving LOCC $\mathcal{T}_{\mathbf{xy}}$ (this is always possible for any quantum channel[15]). If we perform this operation for all the edges, we then define the simulation of the network $\sigma(\mathcal{N}) = \{\sigma_{\mathbf{xy}}\}_{(\mathbf{x},\mathbf{y})\in E}$ where each channel is replaced by a corresponding resource state. If the channels are bosonic, then the simulation is typically asymptotic of the type $\mathcal{E}_{\mathbf{xy}}(\rho) = \lim_\mu \mathcal{E}_{\mathbf{xy}}^\mu(\rho)$ where $\mathcal{E}_{\mathbf{xy}}^\mu(\rho) = \mathcal{T}_{\mathbf{xy}}^\mu(\rho \otimes \sigma_{\mathbf{xy}}^\mu)$ for some sequence of simulating LOCCs $\mathcal{T}_{\mathbf{xy}}^\mu$ and sequence of resource states $\sigma_{\mathbf{xy}}^\mu$.

Here the parameter μ is usually connected with the energy of the resource state. For instance, if $\mathcal{E}_{\mathbf{xy}}$ is a teleportation-covariant bosonic channel, then the resource state $\sigma_{\mathbf{xy}}^\mu$ is its quasi-Choi matrix $\sigma_{\mathcal{E}_{\mathbf{xy}}}^\mu := \mathcal{I} \otimes \mathcal{E}_{\mathbf{xy}}(\Phi^\mu)$, with Φ^μ being a two-mode squeezed vacuum state (TMSV) state[9] whose parameter $\mu = \bar{n} + 1/2$ is related to the mean number $\bar{n}$ of thermal photons. Similarly, the simulating LOCC $\mathcal{T}_{\mathbf{xy}}^\mu$ is a Braunstein-Kimble protocol[67,68] where the ideal Bell detection is replaced by the finite-energy projection onto α-displaced TMSV states $D(\alpha)\Phi^\mu D(-\alpha)$, with D being the phase-space displacement operator[9].

Given an asymptotic simulation of a quantum channel, the associated simulation error is correctly quantified by employing the energy-constrained diamond distance[15], which must go to zero in the limit, i.e.,

$$\left\|\mathcal{E}_{\mathbf{xy}} - \mathcal{E}_{\mathbf{xy}}^\mu\right\|_{\diamond \bar{N}} \xrightarrow{\mu} 0 \text{ for any finite } \bar{N}. \tag{42}$$

Recall that, for any two bosonic channels $\mathcal{E}$ and $\mathcal{E}'$, this quantity is defined as

$$\|\mathcal{E} - \mathcal{E}'\|_{\diamond \bar{N}} := \sup_{\rho_{AB} \in D_{\bar{N}}} \left\|\mathcal{I}_A \otimes \mathcal{E}(\rho_{AB}) - \mathcal{I}_A \otimes \mathcal{E}'(\rho_{AB})\right\|_1, \tag{43}$$

where $D_{\bar{N}}$ is the compact set of bipartite bosonic states with $\bar{N}$ mean number of photons (see ref. [69] for a later and slightly different definition, where the constraint is only on the B part). Thus, in general, if the network has bosonic channels, we may write the asymptotic simulation $\sigma(\mathcal{N}) = \lim_\mu \sigma^\mu(\mathcal{N})$ where $\sigma^\mu(\mathcal{N}) := \{\sigma_{\mathbf{xy}}^\mu\}_{(\mathbf{x},\mathbf{y})\in E}$.

Stretching of the network. Once we simulate a network, the next step is its stretching, which is the complete adaptive-to-block simplification of its output state (for the exact details of this procedure see Supplementary Note 3). As a result of stretching, the n-use output state of the generic network protocol can be decomposed as

$$\rho_{\mathbf{ab}}^n = \bar{\Lambda}_{\mathbf{ab}}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in E} \sigma_{\mathbf{xy}}^{\otimes n_{\mathbf{xy}}}\right], \tag{44}$$

where $\bar{\Lambda}$ represents a trace-preserving LOCC (which is local with respect to Alice and Bob). The LOCC $\bar{\Lambda}$ includes all the adaptive LOCCs from the original protocol besides the simulating LOCCs. In Eq. (44), the parameter $n_{\mathbf{xy}}$ is the number of uses of the edge $(\mathbf{x}, \mathbf{y})$, that we may always approximate to an integer for large n. We have $n_{\mathbf{xy}} \leq n$ for single-path routing, and $n_{\mathbf{xy}} = n$ for flooding protocols in multi-path routing.

In the presence of bosonic channels and asymptotic simulations, we modify Eq. (44) into the approximate stretching

$$\rho_{\mathbf{ab}}^{n,\mu} = \bar{\Lambda}_{\mathbf{ab}}^\mu\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in E} \sigma_{\mathbf{xy}}^{\mu\otimes n_{\mathbf{xy}}}\right], \tag{45}$$

which tends to the actual output $\rho_{\mathbf{ab}}^n$ for large μ. In fact, using a "peeling" technique[15,16] which exploits the triangle inequality and the monotonicity of the trace distance under completely-positive trace-preserving maps, we may write the following bound

$$\left\|\rho_{\mathbf{ab}}^n - \rho_{\mathbf{ab}}^{n,\mu}\right\|_1 \leq \varepsilon^\mu := \sum_{(\mathbf{x},\mathbf{y})\in E} n_{\mathbf{xy}}\left\|\mathcal{E}_{\mathbf{xy}} - \mathcal{E}_{\mathbf{xy}}^\mu\right\|_{\diamond \bar{N}}, \tag{46}$$

which goes to zero in μ for any finite input energy $\bar{N}$, finite number of uses n of the protocol, and finite number of edges $|E|$ in the network (the explicit steps of the proof can be found in Supplementary Note 3).

Stretching with respect to entanglement cuts. The decomposition of the output state can be greatly simplified by introducing cuts in the network. In particular, we may drastically reduce the number of resource states in its representation. Given a cut C of $\mathcal{N}$ with cut-set $\tilde{C}$, we may in fact stretch the network with respect to that specific cut (see again Supplementary Note 3 for exact details of the procedure). In this way, we may write

$$\rho_{\mathbf{ab}}^n(C) = \bar{\Lambda}_{\mathbf{ab}}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in \tilde{C}} \sigma_{\mathbf{xy}}^{\otimes n_{\mathbf{xy}}}\right], \tag{47}$$

where $\bar{\Lambda}_{\mathbf{ab}}$ is a trace-preserving LOCC with respect to Alice and Bob (differently from before, this LOCC now depends on the cut C, but we prefer not to complicate the notation). Similarly, in the presence of bosonic channels, we may consider the

approximate decomposition

$$\rho_{\mathbf{ab}}^{n,\mu}(C)=\bar{\Lambda}_{\mathbf{ab}}^{\mu}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in\tilde{C}}\sigma_{\mathbf{xy}}^{\mu\otimes n_{\mathbf{xy}}}\right], \tag{48}$$

which converges in trace distance to $\rho_{\mathbf{ab}}^{n}(C)$ for large μ.

Data processing and subadditivity. Let us combine the stretching in Eq. (47) with two basic properties of the entanglement measure E_{M}. The first property is the monotonicity of E_{M} under trace-preserving LOCCs; the second property is the subadditivity of E_{M} over tensor-product states. Using these properties, we can simplify the general upper bound of Eq. (41) into a simple and computable single-letter quantity. In fact, for any cut C of the network $\mathcal{N}$, we write

$$E_{\mathrm{M}}[\rho_{\mathbf{ab}}^{n}(C)]\leq E_{\mathrm{M}}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in\tilde{C}}\sigma_{\mathbf{xy}}^{\otimes n_{\mathbf{xy}}}\right] \tag{49}$$

$$\leq\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}n_{\mathbf{xy}}E_{\mathrm{M}}(\sigma_{\mathbf{xy}}), \tag{50}$$

where $\bar{\Lambda}_{\mathbf{ab}}$ has disappeared. Let us introduce the probability of using the generic edge $(\mathbf{x},\mathbf{y})$

$$p_{\mathbf{xy}}:=\lim_{n}\frac{n_{\mathbf{xy}}}{n}, \tag{51}$$

so that we may write the limit

$$\lim_{n}\frac{E_{\mathrm{M}}[\rho_{\mathbf{ab}}^{n}(C)]}{n}\leq\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}p_{\mathbf{xy}}E_{\mathrm{M}}(\sigma_{\mathbf{xy}}). \tag{52}$$

Using the latter in Eq. (41) allows us to write the following bound, for any cut C

$$E_{\mathrm{M}}^{\star}(\mathcal{N})\leq E_{\mathrm{M}}^{\star}(\mathcal{N},C):=\sup_{\{p_{\mathbf{xy}}\}}\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}p_{\mathbf{xy}}E_{\mathrm{M}}(\sigma_{\mathbf{xy}}). \tag{53}$$

In the case of bosonic channels and asymptotic simulations, we may use the triangle inequality

$$\left\|\rho_{\mathbf{ab}}^{n,\mu}-\phi^{n}\right\|_{1}\leq\left\|\rho_{\mathbf{ab}}^{n,\mu}-\rho_{\mathbf{ab}}^{n}\right\|_{1}+\left\|\rho_{\mathbf{ab}}^{n}-\phi^{n}\right\|_{1}\leq\varepsilon^{\mu}+\varepsilon:=\Sigma^{\mu}\to 0. \tag{54}$$

Then, we may repeat the derivations around Eqs. (39)–(41) for $\rho_{\mathbf{ab}}^{n,\mu}$ instead of $\rho_{\mathbf{ab}}^{n}$, where we also include the use of a suitable truncation of the states via a trace-preserving LOCC $\boldsymbol{T}$ (see also Sec. VIII.D of ref. [16] for a similar approach in the point-to-point case). This leads to the μ-dependent upper-bound

$$E_{\mathrm{M}}^{\star}(\mathcal{N},\mu):=\sup_{\mathcal{P}}\lim_{n}\frac{E_{\mathrm{M}}(\rho_{\mathbf{ab}}^{n,\mu})}{n}. \tag{55}$$

Because this is valid for any μ, we may conservatively take the inferior limit in μ and consider the upper bound

$$E_{\mathrm{M}}^{\star}(\mathcal{N}):=\liminf_{\mu}E_{\mathrm{M}}^{\star}(\mathcal{N},\mu). \tag{56}$$

Finally, by introducing the stretching of Eq. (48) with respect to an entanglement cut C, and using the monotonicity and subadditivity of E_{M} with respect to the decomposition of $\rho_{\mathbf{ab}}^{n,\mu}(C)$, we may repeat the previous reasonings and write

$$E_{\mathrm{M}}^{\star}(\mathcal{N})\leq E_{\mathrm{M}}^{\star}(\mathcal{N},C):=\sup_{\{p_{\mathbf{xy}}\}}\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}p_{\mathbf{xy}}\left[\liminf_{\mu}E_{\mathrm{M}}(\sigma_{\mathbf{xy}}^{\mu})\right], \tag{57}$$

which is a direct extension of the bound in Eq. (53).

We may formulate both Eqs. (53) and (57) in a compact way if we define the entanglement measure E_{M} over an asymptotic state $\sigma:=\lim_{\mu}\sigma^{\mu}$ as

$$E_{\mathrm{M}}(\sigma):=\liminf_{\mu}E_{\mathrm{M}}(\sigma^{\mu}). \tag{58}$$

It is clear that, for a physical (non-asymptotic) state, we have the trivial sequence $\sigma^{\mu}=\sigma$ for any μ, so that Eq. (58) provides the standard definition. In the specific case of REE, we may write

$$E_{\mathrm{R}}(\sigma)=\liminf_{\mu}E_{\mathrm{R}}(\sigma^{\mu})=\inf_{\gamma^{\mu}}\liminf_{\mu}S(\sigma^{\mu}||\gamma^{\mu}), \tag{59}$$

where γ^{μ} is a sequence of separable states that converges in trace norm; this means that there exists a separable state γ such that $\|\gamma^{\mu}-\gamma\|_{1}\overset{\mu}{\to}0$. Employing the extended definition of Eq. (58), we may write Eq. (53) for both non-asymptotic $\sigma_{\mathbf{xy}}$ and asymptotic states $\sigma_{\mathbf{xy}}:=\lim_{\mu}\sigma_{\mathbf{xy}}^{\mu}$.

Minimum entanglement cut and upper bounds. By minimizing Eq. (53) over all possible cuts of the network, we find the tightest upper bound, i.e.,

$$E_{\mathrm{M}}^{\star}(\mathcal{N})\leq\min_{C}E_{\mathrm{M}}^{\star}(\mathcal{N},C). \tag{60}$$

Let us now specify this formula for different types of routing. For single-path routing, we have $p_{\mathbf{xy}}\leq 1$, so that we may use

$$\sup_{\{p_{\mathbf{xy}}\}}\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}p_{\mathbf{xy}}(\cdots)\leq\max_{(\mathbf{x},\mathbf{y})\in\tilde{C}}(\cdots), \tag{61}$$

in Eq. (53). Therefore, we derive the following upper bound for the single-path SKC

$$\mathcal{K}(\mathcal{N})\leq\min_{C}E_{\mathrm{M}}(C), \tag{62}$$

where we introduce the single-edge flow of entanglement through the cut

$$E_{\mathrm{M}}(C):=\max_{(\mathbf{x},\mathbf{y})\in\tilde{C}}E_{\mathrm{M}}(\sigma_{\mathbf{xy}}). \tag{63}$$

In particular, we may specify this result to a single chain of N points and $N+1$ channels $\{\mathcal{E}_i\}$ with resource states $\{\sigma_i\}$. This is a quantum network with a single route, so that the cuts can be labeled by i and the cut-sets are just composed of a single edge. Therefore, Eqs. (62) and (63) become

$$\mathcal{K}(\{\mathcal{E}_i\})\leq\min_{i}E_{\mathrm{M}}(\sigma_i). \tag{64}$$

For multi-path routing, we have $p_{\mathbf{xy}}=1$ (flooding), so that we may simplify

$$\sup_{\{p_{\mathbf{xy}}\}}\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}p_{\mathbf{xy}}(\cdots)=\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}(\cdots), \tag{65}$$

in Eq. (53). Therefore, we can write the following upper bound for the multi-path SKC

$$\mathcal{K}^{\mathrm{m}}(\mathcal{N})\leq\min_{C}E_{\mathrm{M}}^{\mathrm{m}}(C), \tag{66}$$

where we introduce the multi-edge flow of entanglement through the cut

$$E_{\mathrm{M}}^{\mathrm{m}}(C):=\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}E_{\mathrm{M}}(\sigma_{\mathbf{xy}}). \tag{67}$$

In these results, the definition of $E_{\mathrm{M}}(\sigma_{\mathbf{xy}})$ is implicitly meant to be extended to asymptotic states, according to Eq. (58). Then, note that the tightest values of the upper bounds are achieved by extending the minimization to all network simulations $\sigma(\mathcal{N})$, i.e., by enforcing $\min_{C}\to\min_{\sigma(\mathcal{N})}\min_{C}$ in Eqs. (62) and (66).

Specifying Eqs. (62), (64), and (66) to the REE, we get the single-letter upper bounds

$$\mathcal{C}(\{\mathcal{E}_i\})\leq\mathcal{K}(\{\mathcal{E}_i\})\leq\min_{i}E_{\mathrm{R}}(\sigma_i), \tag{68}$$

$$\mathcal{C}(\mathcal{N})\leq\mathcal{K}(\mathcal{N})\leq\min_{C}E_{\mathrm{R}}(C), \tag{69}$$

$$\mathcal{C}^{\mathrm{m}}(\mathcal{N})\leq\mathcal{K}^{\mathrm{m}}(\mathcal{N})\leq\min_{C}E_{\mathrm{R}}^{\mathrm{m}}(C), \tag{70}$$

which are Eqs. (4), (11) and (17) of the main text. The proofs of these upper bounds in terms of the REE can equivalently be done following the "converse part" derivations in Supplementary Note 1 (for chains), Supplementary Note 4 (for networks under single-path routing), and Supplementary Note 5 (for networks under multi-path routing). Differently from what presented in this Methods section, such proofs exploit the lower semi-continuity of the quantum relative entropy[8] in order to deal with asymptotic simulations (e.g., for bosonic channels).

Lower bounds. To derive lower bounds we combine the known results on two-way assisted capacities[15] with classical results in network information theory. Consider the generic two-way assisted capacity $\mathcal{C}_{\mathbf{xy}}$ of the channel $\mathcal{E}_{\mathbf{xy}}$ (in particular, this can be either $D_2=Q_2$ or K). Then, using the cut property of the widest path (Supplementary Note 4), we derive the following achievable rate for the generic single-path capacity of the network $\mathcal{N}$

$$\mathcal{C}(\mathcal{N})\geq\min_{C}\max_{(\mathbf{x},\mathbf{y})\in\tilde{C}}\mathcal{C}_{\mathbf{xy}}. \tag{71}$$

For a chain $\{\mathcal{E}_i\}$, this simply specifies to

$$\mathcal{C}(\{\mathcal{E}_i\})\geq\min_{i}\mathcal{C}(\mathcal{E}_i). \tag{72}$$

Using the classical max-flow min-cut theorem (Supplementary Note 5), we derive the following achievable rate for the generic multi-path capacity of $\mathcal{N}$

$$\mathcal{C}^{\mathrm{m}}(\mathcal{N})\geq\min_{C}\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}\mathcal{C}_{\mathbf{xy}}. \tag{73}$$

Simplifications for teleportation-covariant and distillable networks. Recall that a quantum channel $\mathcal{E}$ is said to be teleportation-covariant[15] when, for any teleportation unitary U (Weyl-Pauli operator in finite dimension or phase-space displacement in infinite dimension), we have

$$\mathcal{E}(U\rho U^{\dagger})=V\mathcal{E}(\rho)V^{\dagger}, \tag{74}$$

for some (generally-different) unitary transformation V. In this case the quantum channel can be simulated by applying teleportation over its Choi matrix $\sigma_{\mathcal{E}}:=\mathcal{I}\otimes\mathcal{E}(\Phi)$, where Φ is a maximally-entangled state. Similarly, if the

teleportation-covariant channel is bosonic, we can write an approximate simulation by teleporting over the quasi-Choi matrix $\sigma_{\mathcal{E}}^{\mu} := \mathcal{I} \otimes \mathcal{E}(\Phi^{\mu})$, where Φ^{μ} is a TMSV state. For a network of teleportation-covariant channels, we therefore use teleportation to simulate the network, so that the resource states in the upper bounds of Eqs. (68)–(70) are Choi matrices (physical or asymptotic). In other words, we write the sandwich relations

$$\min_i \mathcal{C}(\mathcal{E}_i) \leq \mathcal{C}(\{\mathcal{E}_i\}) \leq \min_i E_{\mathrm{R}}(\sigma_{\mathcal{E}_i}), \tag{75}$$

$$\min_C \max_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \mathcal{C}_{\mathbf{xy}} \leq \mathcal{C}(\mathcal{N}) \leq \min_C \max_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{R}}(\sigma_{\mathcal{E}_{\mathbf{xy}}}), \tag{76}$$

$$\min_C \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \mathcal{C}_{\mathbf{xy}} \leq \mathcal{C}^{\mathrm{m}}(\mathcal{N}) \leq \min_C \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{R}}(\sigma_{\mathcal{E}_{\mathbf{xy}}}), \tag{77}$$

with the REE taking the form of Eq. (59) on an asymptotic Choi matrix $\sigma_{\mathcal{E}_{\mathbf{xy}}} := \lim_{\mu} \sigma^{\mu}_{\mathcal{E}_{\mathbf{xy}}}$.

As a specific case, consider a quantum channel which is not only teleportation-covariant but also distillable, so that it satisfies[15]

$$\mathcal{C}(\mathcal{E}) = E_{\mathrm{R}}(\sigma_{\mathcal{E}}) = D_1(\sigma_{\mathcal{E}}), \tag{78}$$

where $D_1(\sigma_{\mathcal{E}})$ is the one-way distillability of the Choi matrix $\sigma_{\mathcal{E}}$ (with a suitable asymptotic expression for bosonic Choi matrices[15]). If a network (or a chain) is composed of these channels, then the relations in Eqs. (75)–(77) collapse and we fully determine the capacities

$$\mathcal{C}(\{\mathcal{E}_i\}) = \min_i E_{\mathrm{R}}(\sigma_{\mathcal{E}_i}), \tag{79}$$

$$\mathcal{C}(\mathcal{N}) = \min_C \max_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{R}}(\sigma_{\mathcal{E}_{\mathbf{xy}}}), \tag{80}$$

$$\mathcal{C}^{\mathrm{m}}(\mathcal{N}) = \min_C \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{R}}(\sigma_{\mathcal{E}_{\mathbf{xy}}}). \tag{81}$$

These capacities correspond to Eqs. (7), (14), and (19) of the main text. They are explicitly computed for chains and networks composed of lossy channels, quantum-limited amplifiers, dephasing and erasure channels in Table 1 of the main text.

Regularizations and other measures. It is worth noticing that some of the previous formulas can be re-formulated by using the regularization of the entanglement measure, i.e.,

$$E_{\mathrm{M}}^{\infty}(\sigma) := \lim_n \frac{E_{\mathrm{M}}(\sigma^{\otimes n})}{n}. \tag{82}$$

In fact, let us go back to the first upper bound in Eq. (49), which implies

$$E_{\mathrm{M}}[\rho^n_{\mathbf{ab}}(C)] \leq \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{M}}(\sigma_{\mathbf{xy}}^{\otimes n_{\mathbf{xy}}}). \tag{83}$$

For a network under multi-path routing we have $n_{\mathbf{xy}} = n$, so that we may write

$$\lim_n \frac{E_{\mathrm{M}}[\rho^n_{\mathbf{ab}}(C)]}{n} \leq \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{M}}^{\infty}(\sigma_{\mathbf{xy}}). \tag{84}$$

By repeating previous steps, the latter equation implies the upper bound

$$\mathcal{K}^{\mathrm{m}}(\mathcal{N}) \leq \min_C \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{M}}^{\infty}(\sigma_{\mathbf{xy}}), \tag{85}$$

which is generally tighter than the result in Eqs. (66) and (67). The same regularization can be written for a chain $\{\mathcal{E}_i\}$, which can also be seen as a single-route network satisfying the flooding condition $n_{\mathbf{xy}} = n$. Therefore, starting from the condition of Eq. (83) with $n_{\mathbf{xy}} = n$, we may write

$$\mathcal{K}(\{\mathcal{E}_i\}) \leq \min_i E_{\mathrm{M}}^{\infty}(\sigma_i), \tag{86}$$

which is generally tighter than the result in Eq. (64). These regularizations are important for the REE, but not for the squashed entanglement which is known to be additive over tensor-products, so that $E_{\mathrm{SQ}}^{\infty}(\sigma) = E_{\mathrm{SQ}}(\sigma)$.

Another extension is related to the use of the relative entropy distance with respect to partial-positive-transpose (PPT) states. This quantity can be denoted by RPPT and is defined by[31]

$$E_{\mathrm{P}}(\sigma) := \inf_{\gamma\in\mathrm{PPT}} S(\sigma||\gamma), \tag{87}$$

with an asymptotic extension similar to Eq. (59) but in terms of converging sequences of PPT states γ^{μ}. The RPPT is tighter than the REE but does not provide an upper bound to the distillable key of a state, but rather to its distillable entanglement. This means that it has normalization $E_{\mathrm{P}}(\varphi^n) \geq nR_n$ on a target maximally-entangled state φ^n with nR_n ebits.

The RPPT is known to be monotonic under the action of PPT operations (and therefore LOCCs); it is continuous and subadditive over tensor-product states.

Therefore, we may repeat the derivation that leads to Eq. (41) but with respect to protocols $\mathcal{P}$ of entanglement distribution. This means that we can write

$$Q_2(\mathcal{N}) = D_2(\mathcal{N}) \leq E_{\mathrm{P}}^{\star}(\mathcal{N}) := \sup_{\mathcal{P}} \lim_n \frac{E_{\mathrm{P}}(\rho^n_{\mathbf{ab}})}{n}. \tag{88}$$

Using the decomposition of the output state $\rho^n_{\mathbf{ab}}$ as in Eqs. (47) and (48), and repeating previous steps, we may finally write

$$D_2(\{\mathcal{E}_i\}) \leq \min_i E_{\mathrm{P}}^{\infty}(\sigma_i) \leq \min_i E_{\mathrm{P}}(\sigma_i),$$

for a chain $\{\mathcal{E}_i\}$ with resource states $\{\sigma_i\}$, and

$$D_2(\mathcal{N}) \leq \min_C \max_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{P}}(\sigma_{\mathbf{xy}}), \tag{89}$$

$$D_2^{\mathrm{m}}(\mathcal{N}) \leq \min_C \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{P}}^{\infty}(\sigma_{\mathbf{xy}}) \leq \min_C \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{P}}(\sigma_{\mathbf{xy}}), \tag{90}$$

for the single- and multi-path entanglement distribution capacities of a quantum network $\mathcal{N}$ with resource states $\sigma(\mathcal{N}) = \{\sigma_{\mathbf{xy}}\}_{(\mathbf{x},\mathbf{y})\in E}$.

Data availability

All data in this paper can be reproduced by using the methodology described.

Code availability

Code is available upon reasonable request to the author.

Received: 2 November 2018 Accepted: 22 March 2019
Published online: 17 May 2019

References

1. Kimble, H. J. The Quantum Internet. *Nature* **453**, 1023–1030 (2008).
2. Van Meter, V. *Quantum Networking* (Wiley, 2014).
3. Pirandola, S. & Braunstein, S. L. Unite to build a quantum internet. *Nature* **532**, 169–171 (2016).
4. Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nature Photon.* **9**, 641–652 (2015).
5. Gisin, N. et al. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
6. Watrous, J. *The theory of quantum information*. (Cambridge University Press, Cambridge, 2018).
7. Nielsen, M. A. & Chuang, I. L. *Quantum computation and quantum information*. (Cambridge University Press, Cambridge, 2002).
8. Holevo, A. *Quantum systems, channels, information: A mathematical introduction*. (De Gruyter, Berlin-Boston, 2012).
9. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).
10. Braunstein, S. L. & van Loock, P. Quantum information theory with continuous variables. *Rev. Mod. Phys.* **77**, 513–577 (2005).
11. Fröhlich, B. et al. Quantum secured gigabit optical access networks. *Sci. Rep.* **5**, 18121 (2015).
12. Bunandar, D. et al. Metropolitan quantum key distribution with silicon photonics. *Phys. Rev. X* **8**, 021009 (2018).
13. García-Patrón, R., Pirandola, S., Lloyd, S. & Shapiro, J. H. Reverse coherent information. *Phys. Rev. Lett.* **102**, 210501 (2009).
14. Pirandola, S., García-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **102**, 050503 (2009).
15. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental Limits of Repeaterless Quantum Communications. *Nature Commun.* **8**, 15043 (2017).
16. Pirandola, S. et al. Theory of channel simulation and bounds for private communication. *Quantum Sci. Technol.* **3**, 035009 (2018).
17. 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).
18. Slepian, P. *Mathematical Foundations of Network Analysis*. (Springer-Verlag, New York, 1968).
19. Cover, T. M. & Thomas, J. A. *Elements of Information Theory*. (Wiley, New Jersey, 2006).
20. El Gamal, A. & Kim, Y.-H. *Network Information Theory* (Cambridge Univ. Press 2011).
21. Schrijver, A. *Combinatorial Optimization*. (Springer-Verlag, Berlin, 2003).
22. Azuma, K., Tamaki, K. & Lo, H.-K. All-photonic quantum repeaters. *Nat. Commun.* **6**, 6787 (2015).
23. Cormen, T., Leiserson, C. & Rivest, R. *Introduction to Algorithms*. (MIT Press, Cambridge, MA, 1990).

24. Pollack, M. The maximum capacity through a network. *Oper. Res.* **8**, 733–736 (1960).
25. Medhi, D. & Ramasamy, K. *Network Routing: Algorithms, Protocols, and Architectures*. Second Edition (Morgan Kaufmann publishers, Cambridge MA, 2018).
26. Harris, T. E. & Ross, F. S. Fundamentals of a Method for Evaluating Rail Net Capacities. *Research Memorandum, Rand Corporation* (1955).
27. Ford, L. R. & Fulkerson, D. R. Maximal flow through a network. *Canadian J. Math.* **8**, 399–404 (1956).
28. Elias, P., Feinstein, A. & Shannon, C. E. A note on the maximum flow through a network. *IRE Trans. Inf. Theory* **2**, 117–119 (1956).
29. Ahuja, R. K., Magnanti, T. L. & Orlin, J. B. *Network Flows: Theory, Algorithms and Applications* (Prentice Hall 1993).
30. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. Secure key from bound entanglement. *Phys. Rev. Lett.* **94**, 160502 (2005).
31. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. General paradigm for distilling classical key from quantum states. *IEEE Trans. Inf. Theory* **55**, 1898–1929 (2009).
32. Cope, T. P. W., Hetzel, L., Banchi, L. & Pirandola, S. Simulation of non-Pauli Channels. *Phys. Rev. A* **96**, 022323 (2017).
33. Laurenza, R. & Pirandola, S. General bounds for sender-receiver capacities in multipoint quantum communications. *Phys. Rev. A* **96**, 032318 (2017).
34. Laurenza, R., Braunstein, S. L. & Pirandola, S. Finite-resource teleportation stretching for continuous-variable systems. *Sci. Rep.* **8**, 15267 (2018).
35. Laurenza, R. et al. Tight finite-resource bounds for private communication over Gaussian channels. Preprint at https://arxiv.org/abs/1808.00608 (2018).
36. Pirandola, S., Laurenza, R. & Lupo, C. Fundamental limits to quantum channel discrimination. Preprint at https://arxiv.org/abs/1803.02834 (2018).
37. Pirandola, S., Laurenza, R. & Banchi, L. Conditional channel simulation. *Ann. Phys.* **400**, 289–302 (2019).
38. Vedral, V. The role of relative entropy in quantum information theory. *Rev. Mod. Phys.* **74**, 197–234 (2002).
39. Vedral, V., Plenio, M. B., Rippin, M. A. & Knight, P. L. Quantifying Entanglement. *Phys. Rev. Lett.* **78**, 2275–2279 (1997).
40. Vedral, V. & Plenio, M. B. Entanglement measures and purification procedures. *Phys. Rev. A.* **57**, 1619–1633 (1998).
41. Hayashi, M., Iwama, K., Nishimura, H., Raymond, R. & Yamashita, S. Quantum network coding. *Lect. Notes. Comput. Sci.* **4393**, 610–621 (2007).
42. Hayashi, M., Owari, M., Kato, G. & Cai, N. Secrecy and robustness for active attacks in secure network coding and its application to network quantum key distribution. Preprint at https://arxiv.org/abs/1703.00723 (2017).
43. Song, S. & Hayashi, M. Secure quantum network code without classical communication. *Proc. IEEE Inf. Theory Workshop 2018 (ITW 2018), Guangzhou, China*, November 25–29, 2018, pp. *126–130*.
44. Van Meter, R. et al. Path selection for quantum repeater. *Networks. Netw. Sci.* **3**, 82–95 (2013).
45. Di Franco, C. & Ballester, D. Optimal path for a quantum teleportation protocol in entangled networks. *Phys. Rew. A* **85**, 010303(R) (2012).
46. Tanenbaum, A. S. & Wetherall, D. J. *Computer Networks* (5th Edition, Pearson, 2010).
47. Orlin, J. B. Max flows in O(nm) time, or better. *STOC'13 Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing*, pp. 765–774 (2013).
48. Edmonds, J. & Karp, R. M. Theoretical improvements in algorithmic efficiency for network flow problems. *J. ACM* **19**, 248–264 (1972).
49. Dinic, E. A. Algorithm for solution of a problem of maximum flow in a network with power estimation. *Soviet Math. Doklady***11**, 1277–1280 (1970).
50. Alon, N. Generating pseudo-random permutations and maximum flow algorithms. *Inf. Processing Lett.* **35**, 201–204 (1990).
51. Ahuja, R. K., Orlin, J. B. & Tarjan, R. E. Improved time bounds for the maximum flow problem. *SIAM J. Comput.* **18**, 939–954 (1989).
52. Cheriyan, J., Hagerup, T. & Mehlhorn, K. Can a maximum flow be computed in O(nm) time? *Proceedings of the 17th International Colloquium on Automata, Languages and Programming*, pp. 235–248 (1990).
53. King, V., Rao, S. & Tarjan, R. A faster deterministic maximum flow algorithm. *J. Algorithms* **17**, 447–474 (1994).
54. Goodenough, K., Elkouss, D. & Wehner, S. Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels. *New J. Phys.* **18**, 063005 (2016).
55. Bennett, C. H., DiVincenzo, D. P. & Smolin, J. A. Capacities of quantum erasure channels. *Phys. Rev. Lett.* **78**, 3217–3220 (1997).
56. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
57. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
58. Pirandola, S. et al. High-rate measurement-device-independent quantum cryptography. *Nature Photon.* **9**, 397–402 (2015).
59. Azuma, K., Mizutani, A. & Lo, H.-K. Fundamental rate-loss trade-off for the quantum internet. *Nat. Commun.* **7**, 13523 (2016).
60. Azuma, K. & Kato, G. Aggregating quantum repeaters for the quantum internet. *Phys. Rev. A* **96**, 032332 (2017).
61. Rigovacca, L. et al. Versatile relative entropy bounds for quantum networks. *New J. Phys.* **20**, 013033 (2018).
62. Cope, T. P. W., Goodenough, K. & Pirandola, S. Converse bounds for quantum and private communication over Holevo-Werner channels. *J. Phys. A: Math. Theor.* **51**, 494001 (2018).
63. Pant, M. et al. Routing entanglement in the quantum internet. Preprint at https://arxiv.org/abs/1708.07142 (2017).
64. Bäuml, S., Azuma, K, Kato, G. & Elkouss, D. Linear programs for entanglement and key distribution in the quantum internet. Preprint at https://arxiv.org/abs/1809.03120 (2018).
65. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
66. Ma, X., Zeng, P. & Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **8**, 031043 (2018).
67. Braunstein, S. L. & Kimble, J. Teleportation of continuous quantum variables. *Phys. Rev. Lett.* **80**, 869–872 (1998).
68. Pirandola, S., Laurenza, R. & Braunstein, S. L. Teleportation simulation of bosonic Gaussian channels: Strong and uniform convergence. *Eur. Phys. J. D* **72**, 162 (2018).
69. Shirokov, M. E. Energy-constrained diamond norms and their use in quantum information theory. *Prob. Inf.Transm.* **54**, 20–33 (2018).

Acknowledgements

This work has been supported by the EPSRC via the 'UK Quantum Communications HUB' (EP/M013472/1) and 'qDATA' (EP/L011298/1), and by the European Union via Continuous Variable Quantum Communications (CiViQ, Project ID: 820466). The author would like to thank Seth Lloyd, Koji Azuma, Bill Munro, Richard Wilson, Edwin Hancock, Rod Van Meter, Marco Lucamarini, Riccardo Laurenza, Thomas Cope, Carlo Ottaviani, Gaetana Spedalieri, Cosmo Lupo, Samuel Braunstein, Saikat Guha and Dirk Englund for feedback and discussions.

Author contributions

S.P. developed the theory, carried out the entire work, and wrote the manuscript.

Additional information

Supplementary information accompanies this paper at https://doi.org/10.1038/s42005-019-0147-3.

Competing interests: The authors declare no competing interests.

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

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