Optimal Performance of a Quantum Network

Stefano Pirandola
Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, United Kingdom

We show that the most general protocol of quantum communication between two end-points of a quantum network with arbitrary topology can be reduced to an ensemble of Choi matrices subject to local operations and classical communication. This is found by using a teleportation-based technique which applies to a wide range of quantum channels both in discrete- and continuous-variable settings, including lossy channels, quantum-limited amplifiers, dephasing and erasure channels. Thanks to this reduction, we compute the optimal rates (capacities) at which two end-points of a quantum network can transmit quantum information, distill entanglement, or distribute secret keys. These capacities are all bounded or equal to a single quantity, that we call the entanglement flux of the network. As a particular case, we derive these optimal rates for the basic paradigm of a linear chain of quantum repeaters. Thus our results establish the ultimate rates for repeater-based and network-assisted quantum communications under the most relevant models of noise and decoherence.

I. INTRODUCTION AND MAIN RESULTS

Quantum information [1–5] is today moving towards practical applications, promising next-generation quantum technologies with performances well beyond the state of the art of the current classical infrastructure. In these advances, quantum communications play a central role. The most developed field is quantum cryptography and, in particular, quantum key distribution (QKD) [6–9] which allows two remote authenticated parties to generate unconditionally secure keys. Indeed this field has been the first to be extended to network implementations [10–15], including the first end-to-end [16, 17] realizations at the metropolitan scale [18–22].

Quantum teleportation [23, 24] is another remarkable protocol of quantum communication. Once two remote parties share enough entanglement, they can use local operations (LOs) and classical communication (CC), briefly called LOCCs, to teleport quantum information from one location to the other. This procedure may form the backbone of a future quantum Internet [25], where quantum information is teleported between different nodes and then subject to local quantum processing. In this regard, hybrid approaches which mix different substrates are believed to be the most promising [24].

Networks are built to connect and deliver services to many users. In the quantum setting, there is also a physical reason: Quantum signals are fragile to loss and noise and, therefore, need to be relayed. Any quantum communication between two parties is affected by a fundamental rate-loss trade-off which limits the performance at increasing distances. As shown in Ref. [26], the maximum rates at which two parties can distribute secret keys, distill entanglement, or transmit quantum information over a lossy channel with transmissivity η are all equal to $\mathcal{C}(\eta) = -\log_2(1-\eta)$, corresponding to about 1.44η bits per channel use at high loss. This limit is achieved by using the most general quantum protocols assisted by unlimited two-way CC and adaptive LOs, so called adaptive LOCCs [26, 27]. The optimization over these protocols defines the (generic) two-way assisted capacity $\mathcal{C}$ of the channel. Depending on the task, this may represent a secret-key capacity, an entanglement distillation capacity or a quantum capacity [28].

In order to overcome the previous limitation, one introduces quantum repeaters [29–42]. For instance, instead of using a single optical fiber (lossy channel) with transmissivity η between Alice and Bob, we can split the fiber in two identical parts introducing a quantum repeater in the middle. The two parts are now lossy channels with higher transmissivities, both equal to $\sqrt{\eta}$. Quantum communication in the single links, Alice-repeater and repeater-Bob, can independently occur at the capacity value $\mathcal{C}(\sqrt{\eta})$. Combining and processing the outcomes of these independent procedures (e.g., classically composing the keys or swapping the distributed entanglement), this value becomes an achievable rate for the entire repeater-assisted quantum communication between Alice and Bob, expressed as bits per repeater use.

Now the basic open problem is the following:

- *Can we make a better use of a quantum repeater?*
- *If yes, what is the optimal achievable rate?*

In fact, we can consider more general protocols where the distribution over the two links is coordinated and assisted by adaptive LOCCs involving all the parties. Before and after each transmission, both Alice, Bob and the repeater may perfom LOs on their quantum systems with the assistance of unlimited two-way CCs. Here we explicitly study this more general strategy and we show that it does not give any advantage: $\mathcal{C}(\sqrt{\eta})$ is not only achievable but also the maximum rate compatible with quantum mechanics. In other words, we show that $\mathcal{C}(\sqrt{\eta})$ is the capacity of the quantum communication assisted by the repeater. This basic result is proven and generalized to communication scenarios of increasing complexity, starting from a linear chain of quantum repeaters, and ending with a quantum network of arbitrary topology.

The main tool for proving our results is the method of teleportation stretching [26, 27]. This technique can

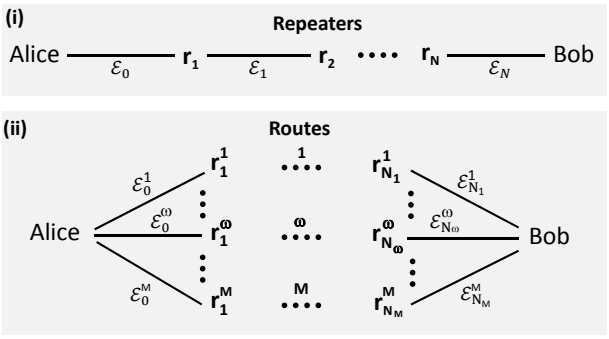

FIG. 1: **Quantum communication scenarios** (i) Linear chain of N quantum repeaters between Alice and Bob, which are connected by an ensemble of $N+1$ quantum channels $\{\mathcal{E}_i\}$. (ii) Quantum network $\mathcal{N}$ where two end-points communicate through a set of M possible routes $\Omega = \{1, \ldots, \omega, \ldots M\}$, each involving a chain of N_ω quantum repeaters. Routes are chosen randomly according to a routing strategy and may have collisions (i.e., a repeater may belong to more routes).

be applied whenever a quantum channel suitably "commutes" with teleportation, in which case the channel is called "stretchable". This is feature of many channels in both continuous variable (CV) and discrete variable (DV) settings, including bosonic Gaussian channels and qubit Pauli channels [27]. Using this method, one can reduce the most general protocol of quantum communication based on adaptive LOCCs. In fact, after n uses of a stretchable channel $\mathcal{E}$, Alice and Bob's output state can be written as $\rho^n_{\mathbf{ab}} = \bar{\Lambda}(\rho^{\otimes n}_{\mathcal{E}})$, where $\rho_{\mathcal{E}}$ is the Choi matrix of the channel [43] and Λ is a trace-preserving LOCC .

Using this decomposition we may bound the two-way assisted capacity of a stretchable channel as

$$\mathcal{C}(\mathcal{E}) \leq \Phi(\mathcal{E}), \tag{1}$$

where $\Phi(\mathcal{E})$ is the entanglement flux of the channel and is defined as the relative entropy of entanglement (REE) of its Choi matrix, $\Phi(\mathcal{E}) := E_R(\rho_{\mathcal{E}})$ [26, 27]. This quantity represents the maximum amount of entanglement that can be transmitted through the channel (as measured by the REE [49]). In particular, for a stretchable channel whose Choi matrix is distillable, we may write [26, 27]

$$\mathcal{C}(\mathcal{E}) = \Phi(\mathcal{E}). \tag{2}$$

Such family of "distillable" channels is very wide and includes lossy (pure-loss) bosonic channels, quantum-limited amplifiers, dephasing and erasure channels.

This technique of teleportation stretching is here extended and applied to network quantum communications. As already mentioned, we start with a linear chain of N quantum repeaters. This is characterized by an ensemble of $N+1$ quantum channels $\{\mathcal{E}_i\}$ describing the sequence of transmissions $i = 0, \ldots, N$ between the end-points (see Fig. 1). We define the entanglement flux of the chain as the minimum of the fluxes

$$\Phi(\{\mathcal{E}_i\}) = \min_i \Phi(\mathcal{E}_i). \tag{3}$$

For a chain of stretchable channels $\{\mathcal{E}_i\}$, we find that the repeater-assisted capacity for the two end-points of the chain, denoted by $\mathcal{C}(\{\mathcal{E}_i\})$, must satisfy the bound

$$\mathcal{C}(\{\mathcal{E}_i\}) \leq \Phi(\{\mathcal{E}_i\}), \tag{4}$$

which is a direct generalization of Eq. (1).

In the case of distillable channels, we then find

$$\mathcal{C}(\{\mathcal{E}_i\}) = \Phi(\{\mathcal{E}_i\}), \tag{5}$$

or, equivalently,

$$\mathcal{C}(\{\mathcal{E}_i\}) = \min_i \mathcal{C}(\mathcal{E}_i). \tag{6}$$

In other words, the repeater-assisted capacity is equal to the minimum among the two-way assisted capacities associated with each channel of the chain.

In optical and telecom communications, the most important type of decoherence is loss. In the case of a chain of repeaters connected by lossy channels with arbitrary transmissivities $\{\eta_i\}$, we can write

$$\mathcal{C}(\{\eta_i\}) = \min_i \mathcal{C}(\eta_i) = \mathcal{C}(\eta_{\min}), \quad \eta_{\min} := \min_i \eta_i \ , \tag{7}$$

or, equivalently,

$$\mathcal{C}(\{\eta_i\}) = -\log_2(1 - \eta_{\min}). \tag{8}$$

Thus, in a lossy bosonic environment, the minimum transmissivity of a chain characterizes the ultimate rate for repeater-based quantum communications, for all the crucial tasks of key generation, entanglement distillation, and transmission of quantum information.

We then consider the general scenario of a quantum network $\mathcal{N}$ with arbitrary topology. We only assume that the quantum channels are memoryless and stretchable. Two end-points of the network, Alice and Bob, are connected by an ensemble of M possible routes $\Omega = \{1, \ldots, \omega, \ldots M\}$ picked with some probability. Each route is a chain of N_ω quantum repeaters connected by $N_\omega + 1$ stretchable channels $\{\mathcal{E}^\omega_i\}$ as shown in Fig. 1.

Remarkably, no matter how complex an adaptive network protocol might be, all the transmissions through the network can be stretched into an ensemble of Choi matrices subject to single and final trace-preserving LOCC. This decomposition allows us to bound the optimal rate performance achievable by the end-points for any of the tasks of key generation, entanglement distillation or transmission of quantum information. In fact, we find that the generic network capacity $\mathcal{C}(\mathcal{N})$ is always bounded by the network version of the entanglement flux. More precisely, define the entanglement flux of the network as the maximum of the fluxes among all the routes connecting the two end-points, i.e.,

$$\Phi(\mathcal{N}) := \max_\omega \Phi_\omega, \quad \Phi_\omega = \min_i \Phi(\mathcal{E}^\omega_i). \tag{9}$$

Then, we may write the simple bound

$$\mathcal{C}(\mathcal{N}) \leq \Phi(\mathcal{N}). \tag{10}$$

In particular, when a quantum network is composed by distillable channels, we have

$$\mathcal{C}(\mathcal{N}) = \Phi(\mathcal{N}), \tag{11}$$

in which case all the network capacities are just equal to the entanglement flux of the network, i.e., the maximum amount of entanglement that can be distributed between the two end-points for each use of the network. In turn, the latter expression leads to

$$\mathcal{C}(\mathcal{N}) = \max_{\omega} \min_{i} \mathcal{C}(\mathcal{E}_i^{\omega}), \tag{12}$$

which is a direct generalization of Eq. (6).

Thus, finding the optimal rate of quantum network is just reduced to solve an extremely simpler classical max-min optimization problem. This remarkable simplification applies to CV networks affected by loss and/or subject to amplification; it also applies to DV networks subject to dephasing or erasure, e.g., spin networks. In general, it also applies to hybrid networks involving any combination of these error models.

For instance, consider a bosonic network where the arbitrary route ω is composed by lossy channels with transmissivities $\{\eta_i^{\omega}\}$. Such lossy channels may represent fibre-based connections or free-space links, at optical or other wavelenghts. Then, the generic network capacity for the end-points of the lossy network reads

$$\mathcal{C}_{\text{loss}}(\mathcal{N}) = -\log_2(1-\tilde{\eta}), \quad \tilde{\eta} := \max_{\omega} \min_{i} \eta_i^{\omega}. \tag{13}$$

This is the ultimate rate, expressed as bits per network use or routed system, at which the end-points can extract secret keys (secret bits), entanglement (ebits) or transmit quantum information (qubits). It is therefore the ultimate limit for any end-to-end quantum communication in a lossy environment.

The manuscript is organized as follows. In Section II, we provide the main tools for the remainder of the paper. In particular, we describe the basics of teleportation stretching, provide the main definitions and briefly review previous literature. In Section III, we study linear chains of quantum repeaters. Then, in Section IV, we analyze the optimal performance of a quantum network with arbitrary topology. Section V is for conclusions.

II. MAIN TOOLS

A. Ideal teleportation and stretchable channels

Let us describe the teleportation protocol in the ideal case, i.e., without noise and with perfect resources and measurements. Given an arbitrary state ρ on some input system a, this is perfectly teleported onto an output system A' by the following procedure. First of all, we need to generate an ideal Einstein-Podolsky-Rosen (EPR) source $\Phi_{AA'}^{\text{EPR}}$ of systems A and A'. For a qudit of dimension d, this is a generalized Bell state

$$\Phi_{AA'}^{\text{EPR}} = d^{-1/2} \sum_{i=1}^{d} |i\rangle_A |i\rangle_{A'}, \tag{14}$$

becoming the usual Bell state $(|00\rangle+|11\rangle)/\sqrt{2}$ for a qubit. For a CV system, we take the asymptotic limit of $d \to +\infty$ in Eq. (14), which corresponds to considering a two-mode squeezed vacuum state [5] with infinite energy.

Then, input system a and EPR system A are subject to an ideal Bell detection. This measurement corresponds to a projection on a basis of Bell states Φ_{aA}^k where the outcome k takes 2^d values for qudits, while it is complex for CVs [24]. More precisely, it is a positive-operator valued measure (POVM) with generic operator

$$\Phi_{aA}^k := (T_k^a \otimes I^A)^{\dagger} \Phi_{aA}^{\text{EPR}} (T_k^a \otimes I^A), \tag{15}$$

where T_k is a teleportation unitary. We call teleportation set $\mathcal{S}$, the ensemble of all teleportation unitaries T_k at dimension d. For a qudit, these are d^2 generalized Pauli operators (generators of a finite-dimensional Weyl-Heisenberg group) [27]; for a CV system, these are an infinite number of displacement operators [5] (infinite-dimensional Weyl-Heisenberg group).

For any given outcome k of the Bell detection on system a and A, the remaining system A' is projected onto $T_k \rho T_k^{\dagger}$ where $T_k \in \mathcal{S}$. The last step is the CC of the outcome k, which allows one to undo the teleportation unitary by applying $T_k^{\dagger}$ to system A'. Note that this process also teleports all correlations that the input system might have with other systems.

Now suppose that system A' is subject to a quantum channel $\mathcal{E}$ which outputs system B. In order to clean the probabilistic action of the Bell measurement, can we apply the correction unitary after the channel? In other words, instead of applying $T_k^{\dagger}$ to system A', can we apply another unitary $U_k^{\dagger}$ to the output system B?

This is not possible in general, but it is a property for a wide class of channels that we call "stretchable".

Definition 1 *We say that a quantum channel $\mathcal{E}$ is "stretchable" by teleportation if, for any $T_k \in \mathcal{S}$ and any input state ρ, we may write*

$$\mathcal{E}(T_k \rho T_k^{\dagger}) = U_k \mathcal{E}(\rho) U_k^{\dagger}, \tag{16}$$

for some unitary U_k.

Typically, the condition of Eq. (16) is satisfied with $U_k \in \mathcal{S}$, i.e., the channel is covariant with the Weyl-Heisenberg group. Notable examples of stretchable channels are all qubit Pauli channels and all bosonic Gaussian channels.

B. Teleportation stretching

Now we show that quantum communication over a stretchable channel can be re-arranged in time, so as to

be reduced to the partial distribution of an ideal EPR source followed by a trace-preserving LOCC. This is the basic idea of the method of "teleportation stretching" (see Fig. 2 for a schematic). Suppose that Alice is sending a quantum system a through a quantum channel $\mathcal{E}$ with output b, i.e., we have $\rho_b = \mathcal{E}(\rho_a)$. We can replace a with another input system A' by quantum teleportation. In fact, we can prepare an ideal EPR source $\Phi_{AA'}^{\text{EPR}}$ of systems A and A', and perform a Bell detection on the original input system a and the EPR system A.

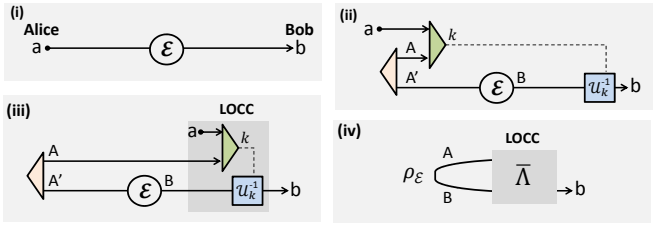

FIG. 2: **Basics of teleportation stretching.** Time flows from left to right. (i) Standard quantum communication through a stretchable channel $\mathcal{E}$ from input system a to output system b. (ii) Input system a is teleported into the new input system A' by a teleportation circuit composed by an ideal EPR state (orange triangle) and a Bell detection (green triangle). The outcome k of the measurement is classically comunicated to Bob who applies an inverse unitary $\mathcal{U}_k^{-1}$. (iii) The ideal EPR source and the Bell detection are stretched in time: The EPR source is anticipated and replaces the original input state, while the Bell detection is postponed after the transmission over the channel. Thus, Alice first distributes the EPR mode A'. Then, a LOCC is applied to the output systems A and B, which includes the previous preparation of system a, the Bell detection, CC of k and the local unitary $\mathcal{U}_k^{-1}$. (iv) The final scheme is equivalent to considering the Choi-matrix $\rho_{\mathcal{E}}$ of the original channel subject to a LOCC.

This leads to perfect teleportation of a onto A', up to a random teleportation unitary, i.e., we have $\rho_{A'} = \mathcal{T}_k(\rho_a) := T_k \rho_a T_k^\dagger$. The unitary $\mathcal{T}_k$ could be erased before transmission through the channel but, because $\mathcal{E}$ is stretchable, $\mathcal{T}_k$ is mapped into an output unitary $\mathcal{U}_k$ that Bob can equivalently delete at the channel output, i.e.,

$$\rho_B = \mathcal{E}(\rho_{A'}) = \mathcal{E} \circ \mathcal{T}_k(\rho_a) = \mathcal{U}_k \circ \mathcal{E}(\rho_a) \ . \qquad (17)$$

Therefore, Bob just needs to receive Alice's CC about the outcome k and correspondingly apply $\mathcal{U}_k^{-1}$ to retrieve the input state, i.e., $\rho_b = \mathcal{U}_k^{-1}(\rho_B) = \mathcal{E}(\rho_a)$.

Thanks to this property, the Bell detection can be delayed in time, meaning that it can equivalently be performed after the transmission through the channel $\mathcal{E}$. The first step then becomes the preparation of the ideal EPR source and the distribution of its system A' through the channel, i.e., we have the shared state $\rho_{AB} = (\mathcal{I} \otimes \mathcal{E})(\Phi_{AA'}^{\text{EPR}})$. Only after this EPR distribution, the Bell detection is applied to system a and EPR system A, performing quantum teleportation of a back in time.

In such a scenario, where the preparation of the EPR source is anticipated and the Bell detection is postponed, Alice and Bob are left with a final LOCC Λ to be applied to their systems A and B. This LOCC combines the preparation of the input system a, the Bell detection, the CC of its outcome k, and the local unitary $\mathcal{U}_k^{-1}$. In other words, we may write Bob's output state as $\rho_b = \Lambda(\rho_{AB})$. Note that, by construction, ρ_{AB} is the Choi matrix $\rho_{\mathcal{E}}$ of the channel $\mathcal{E}$. Thus, we may write $\rho_b = \Lambda(\rho_{\mathcal{E}})$.

Because the final state ρ_b does not depend on k, we may equivalently write $\rho_b = \bar{\Lambda}(\rho_{\mathcal{E}})$, where $\bar{\Lambda}$ is computed from the previous LOCC Λ by averaging over all possible outcomes k of the Bell detection. This is a crucial step because $\bar{\Lambda}$ is not only a LOCC but also a CPTP map, which allows us to exploit the monotonicity of entanglement measures under such maps. As a matter of fact, this method allows us to replace the quantum communication over the channel $\mathcal{E}$ by the Choi-matrix of the channel $\rho_{\mathcal{E}}$ subject to a trace-preserving LOCC. As explained in Ref. [26, 27], this technique is different from programmable quantum gate arrays [44] or port-based teleportation [45]. In particular, the fact that our method provides an overall trace-preserving LOCC is absolutely crucial for the simplification of the adaptive protocols.

C. Teleportation stretching of direct point-to-point quantum communication

Direct point-to-point quantum communication over a stretchable channel can be greatly simplified. Suppose that Alice and Bob are separated by a quantum channel $\mathcal{E}$ and they want to implement the most general protocol with the aim of distributing entanglement, quantum information or secret keys. Suppose that they can exploit unlimited two-way CC and perform real-time adaptive LOs on their systems, i.e., they use adaptive LOCCs. We can always assume that Alice and Bob have countable ensembles of systems, denoted by $\mathbf{a}$ and $\mathbf{b}$, respectively. To simplify notation, we update their local ensembles so that a system a to be transmitted is extracted from the origin ensemble $\mathbf{a} \to \mathbf{a}a$, and a system b received is absorbed by the target ensemble $b\mathbf{b} \to \mathbf{b}$. In general, the quantum communication can be forward or backward: We assume that the parties choose the optimal direction [46].

The most general adaptive protocol goes as follows (here described for forward communication). The first step is the preparation of the initial state of $\mathbf{a}$ and $\mathbf{b}$ by an adaptive LOCC Λ_0. Next, Alice picks a system $a_1 \in \mathbf{a}$ which is sent through the channel $\mathcal{E}$. Once Bob gets the output b_1, the parties apply an adaptive LOCC Λ_1 on all systems $\mathbf{a}b_1\mathbf{b}$. Let us update Bob's set $b_1\mathbf{b} \to \mathbf{b}$. In the second transmission, Alice sends another system $a_2 \in \mathbf{a}$ through $\mathcal{E}$ resulting into an output b_2 for Bob. The parties apply a further adaptive LOCC Λ_2 on all systems $\mathbf{a}b_2\mathbf{b}$. Bob's set is updated and so on. After n transmissions, Alice and Bob share a state $\rho_{\mathbf{ab}}^n$ depending on the sequence of adaptive LOCCs $\mathcal{L} = \{\Lambda_0, \cdots, \Lambda_n\}$.

This adaptive protocol has a rate of R^n if $\|\rho_{\mathbf{ab}}^n - \phi_n\| \leq \varepsilon$, where $\|\cdot\|$ is the trace norm and ϕ_n is a target state

with nR^n bits. By taking the limit of $n \to +\infty$ and optimizing over all the protocols $\mathcal{L}$, one can define the (generic) two-way assisted capacity of the channel

$$\mathcal{C}(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} R^n \ . \tag{18}$$

In particular, if the parties implement entanglement distillation (ED), the target state is a maximally-entangled state and $R^n_{\rm ED}$ is the number of entanglement bits (ebit) per use. If the parties implement QKD, the target state is a private state [47] with secret-key rate $R^n_{\rm K} \geq R^n_{\rm ED}$ [48]. Thus, $\mathcal{C}(\mathcal{E})$ may describe the two-way assisted entanglement distillation capacity D_2 or the secret-key capacity K. Explicitly these capacities are defined as follows

$$D_2(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} R^n_{\rm ED} \leq K(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} R^n_{\rm K}. \tag{19}$$

Also note that $D_2(\mathcal{E}) = Q_2(\mathcal{E})$, where Q_2 is the two-way assisted quantum capacity of the channel. In fact, under unlimited two-way CCs, the transmission of an ebit as part of a qubit and the teleportation of a qubit by means of an ebit are equivalent processes.

We can bound $\mathcal{C}(\mathcal{E})$ using the relative entropy of entanglement (REE) [49]. The REE of state ρ is

$$E_R(\rho) := \min_{\sigma \in \rm SEP} S(\rho||\sigma), \tag{20}$$

where SEP is the set of separable states and

$$S(\rho||\sigma) := \mathrm{Tr}\left[\rho(\log_2 \rho - \log_2 \sigma)\right] \tag{21}$$

is the relative entropy [2]. Then, we may write [26]

$$\mathcal{C}(\mathcal{E}) \leq E_R(\mathcal{E}) := \sup_{\mathcal{L}} \limsup_{n \to +\infty} n^{-1} E_R(\rho^n_{\mathbf{ab}}). \tag{22}$$

As one can check [26], the proof of Eq. (22) derives from

$$\lim_n R^n \leq \lim_n R^n_{\rm K} \leq \limsup_n \ n^{-1} E_R(\rho^n_{\mathbf{ab}}), \tag{23}$$

which is valid for any output state $\rho^n_{\mathbf{ab}}$ asymptotically close to the private state ϕ_n, no matter how $\rho^n_{\mathbf{ab}}$ has been generated. This feature enables us to extend the inequality to other communication scenarios.

The upper bound $E_R(\mathcal{E})$ quantifies the maximum entanglement (as measured by the REE) which can be distributed through the channel by means of general adaptive protocols. Its computation is hard but becomes feasible for stretchable channels. In this case, the most general adaptive protocol can be suitably "stretched" in time and reduced to a non-adaptive protocol where channels are replaced by their Choi matrices and the adaptive LOCCs are all collapsed into a single final trace-preserving LOCC.

Let us describe this procedure. This was originally introduced in Refs. [26, 27] and is given here as a preliminary tool for the next developments. We first discuss the stretching of the ith transmission; then we extend the result by iteration to the entire quantum communication. For simplicity of notation, we omit identities when they are involved in tensor products with other operators. See the panels of Fig. 3 for a schematic.

In Fig. 3(i) we show the ith transmission $a_i \to b_i$ between Alice and Bob. The input state $\rho_{\mathbf{a}a_i\mathbf{b}}$ is subject to the channel $\mathcal{E}$ acting on a_i with the identity being applied to the local ensembles $\mathbf{a}$ and $\mathbf{b}$. After transmission, the adaptive LOCC Λ_i provides the output state $\rho^i_{\mathbf{ab}}$, which is the input for the next transmission. In Fig. 3(ii), we insert an ideal teleportation circuit which teleports a_i into system A'_1. The total state $\sigma := \rho_{\mathbf{a}a_i\mathbf{b}} \otimes \Phi^{\rm EPR}_{A_iA'_i}$ is subject to the Bell detection $B^k_{a_iA_i}(\sigma) := \Phi^k_{a_iA_i}\sigma(\Phi^k_{a_iA_i})^\dagger$, with outcome k. This is equivalent to write $\rho^k_{\mathbf{a}A'_i\mathbf{b}} = \mathcal{T}_k(\rho_{\mathbf{a}a_i\mathbf{b}})$ for a teleportation unitary $\mathcal{T}_k$.

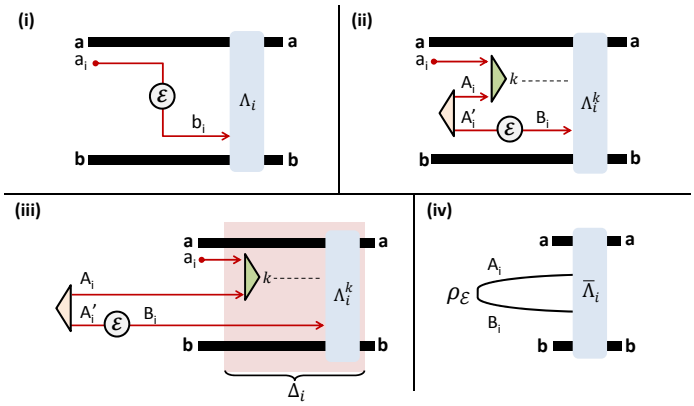

FIG. 3: **Stretching of quantum communication.** Time increases from left to right; Alice is at the top (ensemble $\mathbf{a}$) and Bob is at the bottom (ensemble $\mathbf{b}$). Dashed lines are CC. In panel (i) we show the ith transmission $a_i \to b_i$ through channel $\mathcal{E}$, which is followed by an adaptive LOCC Λ_i performed by the parties on their ensembles $\mathbf{a}$ and $\mathbf{b}$. In panel (ii) we insert an ideal teleportation circuit, just before the channel, teleporting a_1 into the new input A'_1 up to a k-dependent unitary $\mathcal{T}_k$. Since $\mathcal{E}$ is stretchable, this unitary is mapped into an output one $\mathcal{U}_k$ which can be erased by Bob in the next LOCC. In fact, Alice and Bob apply $\Lambda^k_i = \Lambda_i \circ \mathcal{U}^{-1}_k$ where $\mathcal{U}^{-1}_k$ is performed on B_1. In panel (iii) we stretch the protocol by anticipating the distribution of the EPR source and post-poning the Bell detection after the channel. In panel (iv) we show the final result, where the ith transmission through channel $\mathcal{E}$ is replaced by its Choi-matrix $\rho_{\mathcal{E}}$. The tensor product $\rho_{\mathcal{E}} \otimes \rho^{i-1}_{\mathbf{ab}}$ is subject to the trace-preserving LOCC $\bar{\Lambda}_i$.

Applying the quantum channel to the new input system A'_i and using the condition of stretchability, we get

$$\rho^k_{\mathbf{a}B_i\mathbf{b}} := \mathcal{E}(\rho^k_{\mathbf{a}A'_i\mathbf{b}}) = \mathcal{E} \circ \mathcal{T}_k(\rho_{\mathbf{a}a_i\mathbf{b}}) = \mathcal{U}_k \circ \mathcal{E}(\rho_{\mathbf{a}a_i\mathbf{b}}), \tag{24}$$

for some unitary $\mathcal{U}_k$. The value of k is communicated to Bob, who then applies $\mathcal{U}^{-1}_k$ obtaining

$$\rho_{\mathbf{a}B_i\mathbf{b}} = \mathcal{U}^{-1}_k(\rho^k_{\mathbf{a}B_i\mathbf{b}}) = \mathcal{E}(\rho_{\mathbf{a}a_i\mathbf{b}}), \tag{25}$$

which is then transformed into $\rho^i_{\mathbf{ab}}$ by the final LOCC Λ_i. Globally, the parties perform the LOCC $\Lambda^k_i := \Lambda_i \circ \mathcal{U}^{-1}_k$.

Note that we may equivalently write the output as

$$\rho^i_{\mathbf{ab}} = \Lambda^k_i \circ \mathcal{E}_{A'_i} \circ B^k_{a_i A_i}(\sigma) = \Lambda^k_i \circ B^k_{a_i A_i} \circ \mathcal{E}_{A'_i}(\sigma)$$
$$= \Lambda^k_i \circ B^k_{a_i A_i} \left(\rho_{\mathbf{a} a_i \mathbf{b}} \otimes \rho_{\mathcal{E}}^{A_i B_i} \right), \quad (26)$$

where we have commuted the channel and the Bell detection and then used $\rho_{\mathcal{E}}^{A_i B_i} = \mathcal{E}_{A'_i}(\Phi^{\text{EPR}}_{A_i A'_i})$. Let us denote by $\Delta_i := \Lambda^k_i \circ B^k_{a_i A_i}$ the LOs of Alice and Bob. Then, we may write the output state as

$$\rho^i_{\mathbf{ab}} = \Delta_i \left(\rho_{\mathbf{a} a_i \mathbf{b}} \otimes \rho_{\mathcal{E}}^{A_i B_i} \right), \quad (27)$$

which is the scenario depicted in Fig. 3(iii). Since the input state is the output of the previous transmission, i.e., $\rho_{\mathbf{a} a_i \mathbf{b}} = \rho^{i-1}_{\mathbf{ab}}$, we have $\rho^i_{\mathbf{ab}} = \Delta_i(\rho^{i-1}_{\mathbf{ab}} \otimes \rho_{\mathcal{E}}^{A_i B_i})$.

Finally, note that the output state equals its average over the outcomes, i.e., $\rho^i_{\mathbf{ab}} = \sum_k p_k \rho^i_{\mathbf{ab}}$, which leads to

$$\rho^i_{\mathbf{ab}} = \bar{\Lambda}_i(\rho^{i-1}_{\mathbf{ab}} \otimes \rho_{\mathcal{E}}^{A_i B_i}), \quad (28)$$

where $\bar{\Lambda}_i := \sum_k p_k \Delta_i$ is a trace-preserving LOCC. This is the final scenario depicted in Fig. 3(iv).

By using Eq. (28) we can now stretch all the quantum communication in an iteratively way, i.e., transmission after transmission. For instance, consider two transmissions ($n = 2$) as also depicted in Fig. 4. For the first transmission we may write

$$\rho^1_{\mathbf{ab}} = \bar{\Lambda}_1(\rho^0_{\mathbf{ab}} \otimes \rho_{\mathcal{E}}^{A_1 B_1}), \quad (29)$$

where $\rho^0_{\mathbf{ab}} = \Lambda_0(\rho_{\mathbf{a}} \otimes \rho_{\mathbf{b}})$ is the separable input state of Alice's and Bob's ensembles. Because $\rho^0_{\mathbf{ab}}$ is separable, we may insert this preparation into the LOCC and write $\rho^1_{\mathbf{ab}} = \bar{\Lambda}_1(\rho_{\mathcal{E}}^{A_1 B_1})$. This is now the input of the second transmission, for which we may write

$$\rho^2_{\mathbf{ab}} = \bar{\Lambda}_2(\rho^1_{\mathbf{ab}} \otimes \rho_{\mathcal{E}}^{A_2 B_2}) = \bar{\Lambda}_2 \left[\bar{\Lambda}_1(\rho_{\mathcal{E}}^{A_1 B_1}) \otimes \rho_{\mathcal{E}}^{A_2 B_2} \right]$$
$$= \bar{\Lambda}_2 \circ \bar{\Lambda}_1 \left(\rho_{\mathcal{E}}^{A_1 B_1} \otimes \rho_{\mathcal{E}}^{A_2 B_2} \right), \quad (30)$$

since $\bar{\Lambda}_1$ acts as an identity on the second Choi matrix $\rho_{\mathcal{E}}^{A_2 B_2}$. Thus, we finally get $\rho^2_{\mathbf{ab}} = \bar{\Lambda}(\rho_{\mathcal{E}}^{\otimes 2})$, for a trace-preserving LOCC $\bar{\Lambda} = \bar{\Lambda}_2 \circ \bar{\Lambda}_1$.

The extension to arbitrary n transmissions is easy. We may directly iterate Eq. (28) for n times to get

$$\rho^n_{\mathbf{ab}} = (\bar{\Lambda}_n \circ \cdots \circ \bar{\Lambda}_1)(\rho^0_{\mathbf{ab}} \otimes \rho_{\mathcal{E}}^{\otimes n}). \quad (31)$$

Because $\rho^0_{\mathbf{ab}}$ is separable and $\bar{\Lambda}_i$ are all trace-preserving LOCCs, we may equivalently write $\rho^n_{\mathbf{ab}} = \bar{\Lambda}\left(\rho_{\mathcal{E}}^{\otimes n}\right)$, where all the use of the channel are represented by corresponding Choi matrices and all the adaptive LOCCs are collapsed into a single final trace-preserving LOCC $\bar{\Lambda}$. Thus, we have the following

Lemma 2 ([26, 27]) *An adaptive protocol over n uses of a stretchable channel $\mathcal{E}$ reduces to n Choi matrices $\rho_{\mathcal{E}}$ plus a trace-preserving LOCC $\bar{\Lambda}$, i.e., the output reads*

$$\rho^n_{\mathbf{ab}} = \bar{\Lambda}\left(\rho_{\mathcal{E}}^{\otimes n}\right). \quad (32)$$

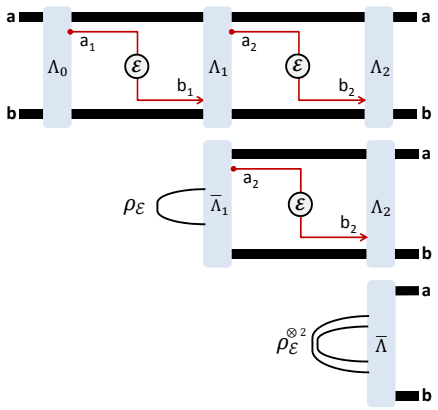

FIG. 4: **Iterative stretching of quantum communication.** Example for $n = 2$ transmissions. See text for details.

Now the combination of Eqs. (22) and (32) leads to a computable upper bound for all the two-way assisted capacities. In fact, define the entanglement flux $\Phi(\mathcal{E})$ of channel $\mathcal{E}$ as the REE of its Choi matrix [27], i.e.,

$$\Phi(\mathcal{E}) := E_R(\rho_{\mathcal{E}}). \quad (33)$$

For stretchable $\mathcal{E}$ we may write [27]

$$\mathcal{C}(\mathcal{E}) \leq E_R(\mathcal{E}) \leq \Phi(\mathcal{E}). \quad (34)$$

This comes from the fact that the REE is non-increasing under trace-preserving LOCC and subadditive on tensor products, so that

$$E_R(\rho^n_{\mathbf{ab}}) = E_R\left[\bar{\Lambda}\left(\rho_{\mathcal{E}}^{\otimes n}\right)\right] \leq n E_R(\rho_{\mathcal{E}}) = n\Phi(\mathcal{E}). \quad (35)$$

Replacing this equation into Eq. (22), one gets Eq. (34).

D. Distillable channels

The entanglement flux is therefore an upper bound for all the two-way assisted capacities $\mathcal{C} = Q_2$, D_2 or K of a stretchable channel. By showing its coincidence with lower bounds based on the coherent information [50, 51] and the reverse coherent information [52, 53], we can determine the two-way assisted capacities of a number of basic quantum channels. These "good" channels may be called "distillable channels" and are defined below.

Let us denote by $I_{(R)C}(\mathcal{E})$ the (reverse) coherent information of a channel $\mathcal{E}$, which is defined as the (reverse) coherent information associated with the channel $\mathcal{E}$ and its Choi matrix $\rho_{AB} = (\mathcal{I} \otimes \mathcal{E})(\Phi^{\text{EPR}}_{AA'}) := \rho_{\mathcal{E}}$. More precisely, we have

$$I_C(\mathcal{E}) := S(\rho_B) - S(\rho_{\mathcal{E}}), \; I_{RC}(\mathcal{E}) := S(\rho_A) - S(\rho_{\mathcal{E}}), \quad (36)$$

where $\rho_{A(B)} := \text{Tr}_{B(A)}(\rho_{AB})$ and $S(\cdot)$ is the von Neumann entropy. These quantities are achievable rates for

entanglement distillation D_1 via one-way CC. In fact, using the hashing inequality [54], we may write

$$\max\{I_C(\mathcal{E}), I_{RC}(\mathcal{E})\} \leq D_1(\rho_{\mathcal{E}}) \leq D_1(\mathcal{E}), \tag{37}$$

where $D_1(\mathcal{E})$ is the one-way assisted entanglement distillation capacity of the channel. Clearly, $D_1(\mathcal{E}) \leq \mathcal{C}(\mathcal{E})$.

Definition 3 *A channel $\mathcal{E}$ is called distillable if it is stretchable and satisfies the additional condition*

$$\max\{I_C(\mathcal{E}), I_{RC}(\mathcal{E})\} = \Phi(\mathcal{E}). \tag{38}$$

Thus, for a distillable channel, all the entanglement that can be transmitted, as given by $\Phi(\mathcal{E})$, is one-way distillable. From Eqs. (37) and (38) we have $\Phi(\mathcal{E}) := E_R(\rho_{\mathcal{E}}) = D_1(\rho_{\mathcal{E}})$, i.e., the Choi matrix of a distillable channel is one-way distillable, with no room for bound entanglement. Most importantly, for a distillable channel, we may write

$$\mathcal{C}(\mathcal{E}) = \Phi(\mathcal{E}) \ . \tag{39}$$

In other words, the entanglement flux of the channel determines all its two-way assisted capacities K, D_2, and Q_2. Furthermore, these rates can be obtained by using protocols based on one-way entanglement distillation.

For a distillable channel, an optimal protocol is a block protocol that goes as follows. Alice prepares n copies of the ideal EPR source $\Phi_{AA'}^{\text{EPR}}$, sending the A'-parts to Bob through the channel, therefore distributing the ensemble of Choi matrices $\rho_{\mathcal{E}}^{\otimes n}$. This is then subject to one-way LOCCs, i.e., LOs and one-way CCs which may be forward or backward. The final state takes the form of Eq. (32) but without the need of performing the stretching of the protocol. It is clear that the output state cannot have any bound entanglement.

It is important to realize that distillable channels form a very wide family. This family includes the lossy (pure-loss) channel with transmissivity $\eta \in [0, 1]$ for which

$$\mathcal{C}_{\text{loss}}(\eta) = -\log_2(1-\eta). \tag{40}$$

Note that this fundamental rate-loss trade-off, found in Ref. [26], was long sought in the literature [53, 55]. Its computation also involved to derive a simple formula for the REE of Gaussian states by adapting techniques from Ref. [56]. Furthermore, $\mathcal{C}_{\text{loss}}(\eta)$ was found to be equal to the maximum quantum discord that can be distributed to the parties, as computed with the techniques of Ref. [57] and confirming the role of discord in QKD [58].

Then, other distillable channels are: The quantum limited amplifier with gain $g \geq 1$, for which [27]

$$\mathcal{C}_{\text{amplifier}}(g) = \log_2[g/(g-1)]. \tag{41}$$

The qubit dephasing channel with probability p, for which we may write [27]

$$\mathcal{C}_{\text{dephasing}}(p) = 1 - H_2(p), \tag{42}$$

where $H_2(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary Shannon entropy [59] (this result can be extended to a qudit in arbitrary dimension [27]). And, finally, the qubit erasure channel with probability p, for which [27, 60]

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

III. CHAIN OF QUANTUM REPEATERS

We have now all the necessary elements to extend the analysis to more complex forms of quantum communication, beyond the basic scenario of a direct connection between Alice and Bob. The first extension is to consider a chain of quantum repeaters between the two parties.

Consider Alice and Bob to be end-points of a linear chain of $N+2$ points with N repeaters in the middle. For $i = 0, \ldots, N$ we assume that point i is connected with point $i+1$ by a quantum channel $\mathcal{E}_i$ which can be forward or backward, for a total of $N+1$ channels $\{\mathcal{E}_0, \ldots \mathcal{E}_i, \ldots \mathcal{E}_N\}$. Each point has a countable ensemble of quantum systems, denoted by $\mathbf{r}_i$ for the i-th point. In particular, we set $\mathbf{a} = \mathbf{r}_0$ for Alice and $\mathbf{b} = \mathbf{r}_{N+1}$ for Bob. To simplify notation, we update the local ensembles so that a system r to be transmitted is extracted from the origin ensemble $\mathbf{r}_i \to \mathbf{r}_i r$, and a system r received is absorbed by the target ensemble $r\mathbf{r}_i \to \mathbf{r}_i$.

The most general distribution protocol over the chain is based on adaptive LOs and unlimited two-way CC involving all the points in the chain. In other words, each point broadcasts classical information and receives classical feedback from all the other points, which is used to perform conditional LOs on the local ensembles. In the following we always assume these "network" adaptive LOCCs, unless we specify otherwise.

The first step is the preparation of the initial state of the local ensembles by a LOCC Λ_0 which provides a separable state $\sigma_{\mathbf{a}\mathbf{r}_1\cdots\mathbf{r}_N\mathbf{b}}$. Then, Alice and the first repeater exchange a quantum system through channel $\mathcal{E}_0$. For a forward transmission, this means that Alice transmits a system $a \in \mathbf{a}$ and the repeater gets its output r with the update $r\mathbf{r}_1 \to \mathbf{r}_1$. For a backward transmission, the repeater transmits a system $r \in \mathbf{r}_1$ and Alice gets a with the update $a\mathbf{a} \to \mathbf{a}$. In each case, this transmission is followed by a LOCC Λ_1 on the local ensembles $\mathbf{a}\mathbf{r}_1\mathbf{r}_2\ldots\mathbf{r}_N\mathbf{b}$. Next, the first and the second repeaters exchange another quantum system through channel $\mathcal{E}_1$ followed by another LOCC Λ_2 applied to all the ensembles, and so on. Finally, Bob exchanges a system with the Nth repeater through channel $\mathcal{E}_N$ and the final LOCC Λ_{N+1} provides the output state $\rho_{\mathbf{a}\mathbf{r}_1\cdots\mathbf{r}_N\mathbf{b}}$.

This procedure completes the exchange of a quantum system through the chain. In the second round, the initial state is the (non-separable) output state of the first round $\sigma^2_{\mathbf{a}\mathbf{r}_1\cdots\mathbf{r}_N\mathbf{b}} = \rho^1_{\mathbf{a}\mathbf{r}_1\cdots\mathbf{r}_N\mathbf{b}}$. The protocol goes as before with each pair of points i and $i+1$ exchanging one system between two LOCCs. The second round ends by giving the output state $\rho^2_{\mathbf{a}\mathbf{r}_1\cdots\mathbf{r}_N\mathbf{b}}$ which is the input for the third

round and so on. After n rounds, all the points share an output state $\rho^n_{\mathbf{ar}_1\cdots\mathbf{r}_N\mathbf{b}}$. By tracing out the repeaters, we get Alice and Bob's final state $\rho^n_{\mathbf{ab}}$. This state is obtained after n uses of the chain $\{\mathcal{E}_i\}$ and depends on the whole sequence of adaptive LOCCs $\mathcal{L}=\{\Lambda_0,\cdots,\Lambda_{n(N+1)}\}$.

The previous adaptive protocol has a rate of R^n if $\|\rho^n_{\mathbf{ab}}-\phi_n\|\leq\varepsilon$, where ϕ_n is a target state with nR^n bits. By taking the limit of $n\to+\infty$ and optimizing over $\mathcal{L}$, we define the (generic) repeater-assisted capacity for the two end-points of the chain, i.e.,

$$\mathcal{C}(\{\mathcal{E}_i\}):=\sup_{\mathcal{L}}\lim_n R^n\ . \tag{44}$$

Let us specify the task of the distribution protocol. For QKD, the target state is a private state [47] with secret key rate R^n_{ED} (bits per chain use). In this case $\mathcal{C}(\{\mathcal{E}_i\})$ describes the repeater-assisted secret key capacity

$$K(\{\mathcal{E}_i\}):=\sup_{\mathcal{L}}\lim_n R^n_{\mathrm{K}}\ . \tag{45}$$

For entanglement distillation (ED), the target state is a maximally-entangled state with rate $R^n_{\mathrm{ED}}\leq R^n_{\mathrm{K}}$ (ebits per chain use). In this other case, $\mathcal{C}(\{\mathcal{E}_i\})$ represents the repeater-assisted entanglement distillation capacity

$$D_2(\{\mathcal{E}_i\}):=\sup_{\mathcal{L}}\lim_n R^n_{\mathrm{ED}}\leq K(\{\mathcal{E}_i\}). \tag{46}$$

Since an ebit can teleport a qubit and a qubit can distribute an ebit, D_2 coincides with the repeater-assisted quantum capacity, i.e., $D_2(\{\mathcal{E}_i\})=Q_2(\{\mathcal{E}_i\})$.

We can build an upper bound for all the previous capacities, i.e., for the generic $\mathcal{C}(\{\mathcal{E}_i\})$. In fact, using the general inequality in Eq. (23), we may write

$$\mathcal{C}(\{\mathcal{E}_i\})\leq E_R(\{\mathcal{E}_i\}):=\sup_{\mathcal{L}}\limsup_{n\to+\infty}n^{-1}E_R(\rho^n_{\mathbf{ab}}). \tag{47}$$

This upper bound can be extremely simplified in the case of a "stretchable chain", i.e., a chain composed by stretchable channels. It is sufficient to extend the notion of entanglement flux to a chain and then suitably stretch the repeater-based protocol by teleportation.

Recall that the entanglement flux $\Phi(\mathcal{E})$ of a channel $\mathcal{E}$ is defined as the REE of its Choi matrix, i.e., $\Phi(\mathcal{E}):=E_R(\rho_{\mathcal{E}})$. Thus, we may define the entanglement flux of a chain as the minimum flux of its channels

$$\Phi(\{\mathcal{E}_i\}):=\min_i\{\Phi(\mathcal{E}_i)\}\ . \tag{48}$$

For a stretchable chain, this quantity bounds the maximum entanglement that can be distributed between the two end-points and, therefore, bounds all the repeater-assisted capacities. In fact, we have the following

Theorem 4 *Consider a chain of $N+2$ points connected by stretchable channels $\{\mathcal{E}_i\}_{i=0}^N$. The most general adaptive protocol over n uses of the chain provides the output*

$$\rho^n_{\mathbf{ab}}=\bar{\Lambda}_i\left(\rho^{\otimes n}_{\mathcal{E}_i}\right)\quad \textit{for any } i, \tag{49}$$

where $\bar{\Lambda}_i$ is a trace-preserving LOCC. As a result, the repeater-assisted capacities are all bounded by the entanglement flux of the chain, i.e.,

$$\mathcal{C}(\{\mathcal{E}_i\})\leq\Phi(\{\mathcal{E}_i\}). \tag{50}$$

Proof. To prove the decomposition in Eq. (49) consider the case of 3-point chain ($N=1$), where Alice $\mathbf{a}$ and Bob $\mathbf{b}$ are connected with a middle repeater $\mathbf{r}$ by means of two stretchable channels $\mathcal{E}$ and $\mathcal{E}'$. This is shown in Fig. 5 for the first two uses of the repeater. The direction of the channels can be different and the extension to arbitrary N is just a matter of technicalities. As depicted in Fig. 5, we can stretch the protocol iteratively. Each time we stretch a transmission between two ensembles, we accumulate a Choi matrix at the input, which distributes entanglement between those two ensembles. Correspondingly, the two adaptive LOCCs (before and after the transmission) are collapsed into a single trace-preserving LOCC, with the output state $\rho_{\mathbf{arb}}$ becoming the input state for the next transmission. After two uses of the repeater we have the output state $\rho^2_{\mathbf{arb}}=\bar{\Lambda}\left(\rho^{\otimes 2}_{\mathcal{E}}\otimes\rho^{\otimes 2}_{\mathcal{E}'}\right)$. By tracing the repeater $\mathbf{r}$, we derive $\rho^2_{\mathbf{ab}}=\bar{\Lambda}_{\mathbf{ab}}\left(\rho^{\otimes 2}_{\mathcal{E}}\otimes\rho^{\otimes 2}_{\mathcal{E}'}\right)$ up to re-defining the LOCC. By extending the procedure to an arbitrary number of repeaters N and uses n, we get

$$\rho^n_{\mathbf{ar}_1\ldots\mathbf{r}_N\mathbf{b}}=\bar{\Lambda}\left(\otimes_{i=0}^N\,\rho^{\otimes n}_{\mathcal{E}_i}\right),\ \rho^n_{\mathbf{ab}}=\bar{\Lambda}_{\mathbf{ab}}\left(\otimes_{i=0}^N\,\rho^{\otimes n}_{\mathcal{E}_i}\right). \tag{51}$$

More details are provided in Appendix A.

From the stretched scenario $\bar{\Lambda}\left(\otimes_i\rho^{\otimes n}_{\mathcal{E}_i}\right)$ which is depicted in Fig. 6, we may consider any two points i and $i+1$ and extend them to consider the bipartition $(\mathbf{a}\cdots\mathbf{r}_i)$ for an "extended Alice" and $(\mathbf{r}_{i+1}\cdots\mathbf{b})$ for an "extended Bob". Then, all the Choi matrices $\rho^{\otimes n}_{\mathcal{E}_k}$ with $k<i$ are included in Alice's LOs and all those with $k>i+1$ are included in Bob's. The result is that we remain with the input $\rho^{\otimes n}_{\mathcal{E}_i}$ which is processed by a corresponding trace-preserving LOCC $\bar{\Lambda}_i$ which outputs $\rho^n_{\mathbf{ab}}$ by tracing out all the repeaters (one key point here is that $\bar{\Lambda}_i$ remains a LOCC with respect to $\mathbf{a}$ and $\mathbf{b}$). This leads to Eq. (49) for any i. Since the REE is non-decreasing under trace-preserving LOCCs and subadditive under tensor products, we may write $E_R(\rho^n_{\mathbf{ab}})\leq nE_R(\rho_{\mathcal{E}_i})$ for any i. Replacing the latter inequality in Eq. (47), we derive $\mathcal{C}(\{\mathcal{E}_i\})\leq E_R(\{\mathcal{E}_i\})\leq E_R(\rho_{\mathcal{E}_i})=\Phi(\mathcal{E}_i)$ for any i, which implies $\mathcal{C}(\{\mathcal{E}_i\})\leq E_R(\{\mathcal{E}_i\})\leq\Phi(\{\mathcal{E}_i\})$. ■

Note that the final stretched scenario depicted in Fig. 6 remains the same if we randomly permute the order of the transmissions in the quantum communication. For instance, in some use of the chain, the first transmission might occur between two repeaters, with the transmission between Alice and the first repeater only occurring at a later time. This permutation-invariance is true proviso that we suitably replace the final trace-preserving LOCC in Eq. (51) and, therefore, in Eq. (49). Thus, the main result in Eq. (50) is valid for any order of the transmissions in the chain.

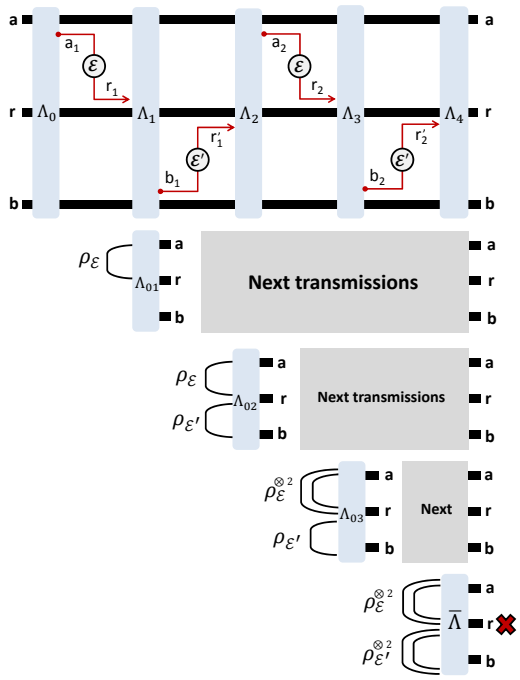

FIG. 5: **Teleportation stretching of a repeater**. The top scheme shows two subsequent uses of the repeater **r** by Alice **a** and Bob **b**, where each use involves the transmissions of two systems $a_k \to r_k$ and $b_k \to r'_k$, through channels $\mathcal{E}$ and $\mathcal{E}'$. Each transmission occurs between two LOCCs. We iterate the method of teleportation stretching to simplify transmission after transmission. At the end we trace the repeater.

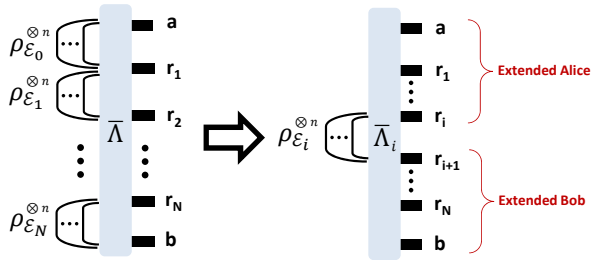

FIG. 6: **Reduction of the stretched scenario**. See text.

Now, by using Theorem 4, we can bound the maximal rates for entanglement distillation (D_2), quantum communication (Q_2) and secret key generation (K) through a stretchable chain of repeaters. It is in fact sufficient to compute the entanglement flux of each individual channel $\Phi(\mathcal{E}_i)$ and take the minimum. Note that the entanglement flux has been analytically computed for many channels in both CV and DVs, including all single-mode Gaussian channels and all Pauli channels [27].

There are important channels for which the entanglement flux exactly coincides with the two-way assisted capacities, i.e., $\Phi(\mathcal{E}) = \mathcal{C}(\mathcal{E})$ with $\mathcal{C} = D_2$, Q_2 or K. As discussed in Section II, this is the case of the distillable channels. For chains involving these channels, i.e., "distillable chains", we establish all the repeater-assisted capacities. We have the following result.

Corollary 5 *Consider a chain of $N+2$ points connected by $N+1$ distillable channels $\{\mathcal{E}_i\}$, which include lossy channels, quantum-limited amplifiers, dephasing or erasure channels. The generic repeater-assisted capacity of the chain is equal to its entanglement flux. In turn, this is equal to the minimum among the two-way assisted capacities of the individual channels*

$$\mathcal{C}(\{\mathcal{E}_i\}) = \Phi(\{\mathcal{E}_i\}) = \min_i \mathcal{C}(\mathcal{E}_i) \ . \tag{52}$$

Proof. For the considered channels, the generic two-way assisted capacity coincides with the entanglement flux, i.e., $\mathcal{C}(\mathcal{E}_i) = \Phi(\mathcal{E}_i)$. Thus, from Theorem 4, we find $\mathcal{C}(\{\mathcal{E}_i\}) \leq \Phi(\{\mathcal{E}_i\}) := \min_i \Phi(\mathcal{E}_i) = \min_i \mathcal{C}(\mathcal{E}_i)$. It is clear that $\min_i \mathcal{C}(\mathcal{E}_i)$ is also an achievable lower-bound for $\mathcal{C}(\{\mathcal{E}_i\})$. In fact, $\mathcal{C}(\mathcal{E}_i)$ is the capacity for the single connection between points i and $i+1$, not assisted by the other points. By composing all the connections, Alice and Bob can communicate with a rate which is at least the minimum of the single-connection capacities. ■

As a result of the previous Corollary, we establish the ultimate rate of repeater-assisted QKD in lossy channels. Suppose that Alice and Bob are connected by N repeaters and each connection $\mathcal{E}_i$ in the chain is a lossy channel with transmissivity η_i. Then, the repeater-assisted secret key capacity of the lossy chain is

$$\begin{aligned} K(\{\eta_i\}) &= \min_i K(\eta_i) = \min_i \left[-\log_2(1-\eta_i)\right] \\ &= -\log_2(1-\eta_{\min}), \quad \eta_{\min} := \min_i \eta_i \ . \end{aligned} \tag{53}$$

No matter how many repeaters we use, the minimum transmissivity in the chain fully determines the ultimate rate of QKD between the two end-points. The same conclusion is reached for entanglement distillation and quantum communication since Eq. (53) is valid for $\mathcal{C}_{\rm loss}(\{\eta_i\})$.

In a chain of bosonic systems connected by amplifiers with gains $\{g_i\}$, the repeater-assisted capacity is determined by the highest gain $g_{\max} := \max_i g_i$, so that

$$\mathcal{C}_{\rm amplifier}(\{g_i\}) = \log_2[g_{\max}/(g_{\max}-1)]. \tag{54}$$

For a spin chain where the state transfer from the ith spin to the next one is modelled by a dephasing channel with probability p_i, we find

$$\mathcal{C}_{\rm dephasing}(\{p_i\}) = 1 - H_2(p_{\max}), \tag{55}$$

where $p_{\max} := \max_i p_i$ and H_2 is the binary Shannon entropy. When the spins are connected by erasure channels with probabilities $\{p_i\}$, then we have

$$\mathcal{C}_{\rm erasure}(\{p_i\}) = 1 - p_{\max}. \tag{56}$$

A. Optimal use of quantum repeaters in lossy optical communications

Let us discuss in more detail the important case of repeaters in a lossy bosonic environment. Suppose that

we are given a long communication line (e.g. a telecom fibre) with transmissivity η plus a number N of repeaters that we could potentially use along the line. Assume that any cut of the line generates two sub-lines which are lossy channels with transmissivities η' and η'' such that $\eta = \eta'\eta''$. The question is: *What is the optimal way to cut the line and insert the repeaters?*

From the formula of the repeater-assisted capacity

$$\mathcal{C}_{\rm loss}(\{\eta_i\}) = -\log_2(1-\eta_{\rm min}), \quad \eta_{\rm min} := \min_i \eta_i \ , \quad (57)$$

we can easily see that the optimal strategy corresponds to N equidistant cuts of the line, so that the resulting $N+1$ lossy channels have identical transmissivities

$$\eta_i = \eta_{\rm min} = \sqrt[N+1]{\eta} \ . \quad (58)$$

This leads to the maximum capacity

$$\mathcal{C}_{\rm loss}(\eta, N) = -\log_2\left(1 - \sqrt[N+1]{\eta}\right) \ . \quad (59)$$

This capacity is plotted in Fig. 7 for increasing number N of equidistant repeaters on the line, whose total loss is expressed in decibel (dB), given by $\eta_{\rm dB} := -10\log_{10}\eta$. In particular, we compare the repeater-based capacity with the fundamental benchmark, i.e., the maximum performance achievable in the absence of repeaters.

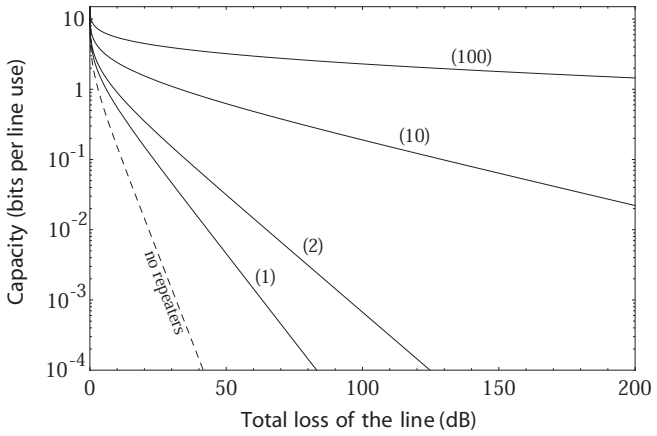

FIG. 7: Capacity (bits per line use) versus total loss in the line (in dB). We first show the maximum performance which is achievable by direct quantum communication with no repeaters on the line (dashed curve). This is the fundamental benchmark to be surpassed by the use of quantum repeaters. This benchmark is then compared with the optimal rates achievable by means of N equidistant repeaters, for $N = 1, 2, 10$ and 100 (solid curves).

Suppose that we require a minimum performance of 1 bit per line use (depending on the specific protocol, this could be 1 secret bit or 1 ebit or 1 qubit per line use). From Eq. (59), we see that we need at least

$$N = \log_2 \frac{1}{\eta} - 1 \simeq 0.332 \ \eta_{\rm dB} - 1 \quad (60)$$

equidistant repeaters. This is about 1 repeater every 6dB loss, corresponding to about 30km in standard optical fibre (at the loss rate of 0.2dB/km).

It is interesting to study two regimes that we may call repeater-dominant and loss-dominant. In the former, we fix the total transmissivity η of the line and use many equidistant repeaters $N \gg 1$. We then have

$$\mathcal{C}_{\rm loss}(\eta, N \gg 1) \simeq \log_2 N - \log_2 \ln \frac{1}{\eta} \ , \quad (61)$$

which means that the capacity scales logarithmically in the number of repeaters, independently from the loss.

In the second regime (loss-dominant), we fix the number of repeaters N and take the limit of high loss $\eta \simeq 0$. We then get

$$\mathcal{C}_{\rm loss}(\eta \simeq 0, N) \simeq \frac{\sqrt[N+1]{\eta}}{\ln 2} \simeq 1.44 \ \sqrt[N+1]{\eta}. \quad (62)$$

In nats, this is equal to $\sqrt[N+1]{\eta}$ nats per line use.

IV. QUANTUM NETWORKS

A. Notation and preliminary definitions

We consider a quantum network $\mathcal{N}$ whose points are connected by memoryless channels. The network can be represented as an undirected graph [61] $\mathcal{N} = (P, E)$ where P is the finite set of points of the network (vertices) and E is the set of all connections (edges). An arbitrary point $x \in P$ has an associated local ensemble of quantum systems $\mathbf{x}$ used for quantum communication. To simplify notation, we identify a point with its local ensemble $x = \mathbf{x}$. Two points $\mathbf{x}, \mathbf{y} \in P$ are connected if there is an edge $(\mathbf{x}, \mathbf{y}) \in E$, i.e., a corresponding channel $\mathcal{E}_{\mathbf{xy}}$ between $\mathbf{x}$ and $\mathbf{y}$ (forward or backward, we implicitly assume the optimal direction). As before, we adopt $\mathbf{a}$ and $\mathbf{b}$ for the two end-points, Alice and Bob, while we use $\mathbf{r}$'s for the repeaters (middle points of the network).

By definition, a route is a path between the two end-points, i.e., an ordered sequence of edges of the type $\{(\mathbf{a}, \mathbf{r}_1), (\mathbf{r}_1, \mathbf{r}_2), \cdots, (\mathbf{r}_N, \mathbf{b})\}$, that we may also denote as $\mathbf{a} - \mathbf{r}_1 - \cdots - \mathbf{r}_N - \mathbf{b}$. Correspondingly, there is a sequence of channels $\{\mathcal{E}_0, \ldots, \mathcal{E}_N\}$ where $\mathcal{E}_i := \mathcal{E}_{\mathbf{r}_i\mathbf{r}_{i+1}}$ with $i = 0, \ldots, N$ and setting $\mathbf{a} = \mathbf{r}_0$ and $\mathbf{b} = \mathbf{r}_{N+1}$. In general, the two end-points are connected by an ensemble of possible routes $\Omega = \{1, \ldots, \omega, \ldots\}$ through which systems can be transmitted. Generic route ω : $\mathbf{a} - \mathbf{r}_1^\omega - \cdots - \mathbf{r}_{N_\omega}^\omega - \mathbf{b}$ involves the transmission through $N_\omega + 1$ channels $\{\mathcal{E}_0^\omega, \ldots, \mathcal{E}_{N_\omega}^\omega\}$. These routes span all the points P of the network and may have collisions, which means that one or more repeaters may be in common to different routes. Finally, as in the case of a linear chain, each transmission is alternated with network LOCCs: These are adaptive LOs performed by all points on their local ensembles, and assisted by unlimited two-way CC involving the entire network.

B. Sequential access of a quantum network

The most general protocol for sequential communication over a quantum network involves the use of generally-different routes, accessed one after the other. The network is initialized by a first LOCC Λ_0 into an initial separable state. Then, with probability π_0^1, Alice $\mathbf{a}$ exchanges one system with repeater $\mathbf{r}_1^1$. This is followed by another LOCC Λ_1. Next, with probability π_1^1, repeater $\mathbf{r}_1^1$ exchanges one system with repeater $\mathbf{r}_2^1$ and so on. Finally, with probability $\pi_{N_1}^1$, repeater $\mathbf{r}_{N_1}^1$ exchanges one system with Bob $\mathbf{b}$, followed by a final LOCC Λ_{N_1+1}. Thus, with probability $p_1 = \Pi_i \pi_i^1$, the end-points exchange one system which has undergone $N_1 + 1$ transmissions $\{\mathcal{E}_i^1\}$ along the first route $\mathbf{a} - \{\mathbf{r}_i^1\} - \mathbf{b}$.

The next uses involve generally-different routes. After a large number n of uses, the random process defines a routing table $\mathcal{R} = \{\omega, p_\omega\}$, where route ω is picked with probability p_ω and involves $N_\omega + 1$ transmissions $\{\mathcal{E}_i^\omega\}$. Thus, we have a total of $N_{\text{tot}} = \Sigma_\omega n p_\omega (N_\omega + 1)$ transmissions and a sequence of LOCCs $\mathcal{L} = \{\Lambda_0, \ldots, \Lambda_{N_{\text{tot}}}\}$, whose output provides Alice and Bob's final state $\rho_{\mathbf{ab}}^n$. Note that we may weaken the previous description: While mantaining the sequential use of the routes, in each route we may permute the order of the transmissions (as before for the case of a linear chain of repeaters).

The sequential network protocol is characterized by $\mathcal{R}$ and $\mathcal{L}$, and its rate is R^n if $\|\rho_{\mathbf{ab}}^n - \phi_n\| \leq \varepsilon$, where ϕ_n is a target state of nR^n bits. The generic network capacity is defined by optimizing the asymptotic rate over all protocols, i.e.,

$$\mathcal{C}(\mathcal{N}) := \sup_{(\mathcal{R},\mathcal{L})} \lim_n R^n. \tag{63}$$

This provides the maximum number of (quantum, entanglement, or secret) bits which are distributed on average for each sequential use of the network, i.e., for each quantum system routed through the network. By specifying the type of target state, we have the corresponding network capacities for quantum communication, entanglement distillation and QKD, which satisfy

$$Q_2(\mathcal{N}) = D_2(\mathcal{N}) \leq K(\mathcal{N}). \tag{64}$$

In the following, we derive a simple upper-bound for these network capacities in the case of a stretchable quantum network, i.e., a quantum network with stretchable channels. Most importantly, they can be exactly computed in the case of a distillable quantum network, i.e., a quantum network connected by distillable channels.

C. Stretchable quantum networks

The stretching of a quantum network is a procedure which directly generalizes that employed for a linear chain of quantum repeaters, with the difference that we now have many chains with possible collisions. Using this method, we derive the following upper bound.

Theorem 6 *Consider a network $\mathcal{N}$ of stretchable channels, where two end-points are connected by an ensemble of routes $\Omega = \{\omega\}$, with each route ω involving transmissions through a sequence of channels $\{\mathcal{E}_i^\omega\}$. The generic network capacity $\mathcal{C}(\mathcal{N})$ is upper-bounded by the entanglement flux of the network $\Phi(\mathcal{N})$, defined as the maximum entanglement flux among the different routes, i.e.,*

$$\mathcal{C}(\mathcal{N}) \leq \Phi(\mathcal{N}) := \max_\omega \Phi_\omega, \quad \Phi_\omega = \min_i \{\Phi(\mathcal{E}_i^\omega)\}. \tag{65}$$

Proof. To show the basic rationale, consider two repeaters on two different routes $\omega = 1, 2$. We have route $1 : \mathbf{a} - \mathbf{r}_1 - \mathbf{b}$ with channels $\{\mathcal{E}_1^1, \mathcal{E}_2^1\}$, and route $2 : \mathbf{a} - \mathbf{r}_2 - \mathbf{b}$ with channels $\{\mathcal{E}_1^2, \mathcal{E}_2^2\}$. The first use of these routes is shown in Fig. 8. Iterative stretching leads to $\rho_{\mathbf{aRb}} = \bar{\Lambda}(\otimes_{\omega,i}\, \rho_{\mathcal{E}_i^\omega})$, where $\mathbf{R} = \mathbf{r}_1\mathbf{r}_2$ are the middle repeaters. As before, just note that the final stretched scenario is permutation-invariant up to re-define the final LOCC, which means that we get an equivalent decomposition of the output state for any re-ordering of the transmissions in the network quantum communication.

Within each route ω we then identify the channel with the minimum entanglement flux, i.e., $\mathcal{E}_\omega$ such that $\Phi(\mathcal{E}_\omega) = \Phi_\omega$. For instance, we suppose they are $\mathcal{E}_1^1$ and $\mathcal{E}_1^2$ in the example of Fig. 8. The key point is that we can stretch the routes only with respect to these channels, while including all the other channels in the network operations. The resulting quantum operation $\tilde{\Lambda}$ applied to the remaining Choi matrices $\otimes_\omega \rho_{\mathcal{E}_\omega}$ is trace-preserving and still local with respect to Alice and Bob. By tracing out all the repeaters, we get the output state $\rho_{\mathbf{ab}} = \Delta\left(\otimes_\omega \rho_{\mathcal{E}_\omega}\right)$ with Δ being a trace-preserving LOCC. This formula can be extended to n uses of the network and an arbitrary routing set where route ω is picked with probability p_ω. It easy to check that this leads to

$$\rho_{\mathbf{ab}}^n = \Delta(\otimes_\omega\, \rho_{\mathcal{E}_\omega}^{\otimes n p_\omega}). \tag{66}$$

Now, for QKD, we may write

$$\begin{aligned} K(\mathcal{N}) &:= \sup_{(\mathcal{R},\mathcal{L})} \lim_n R_{\text{K}}^n \\ &\leq \sup_{(\mathcal{R},\mathcal{L})} \limsup_n n^{-1} E_R(\rho_{\mathbf{ab}}^n), \end{aligned} \tag{67}$$

where we have used Eq. (23). Using the stretched network in Eq. (66) and the properties of the REE, we derive $K(\mathcal{N}) \leq \max_{\mathcal{R}} \Sigma_\omega p_\omega \Phi_\omega \leq \max_{\omega\in\Omega} \Phi_\omega$. This bound applies to all network capacities, proving Eq. (65). ■

D. Distillable quantum networks

Note that Theorem 6 identifies a candidate optimal route for the quantum systems, which is that with maximum entanglement flux. This is indeed the optimal route in a network which is made of distillable channels, such as lossy channels. We have the following result.

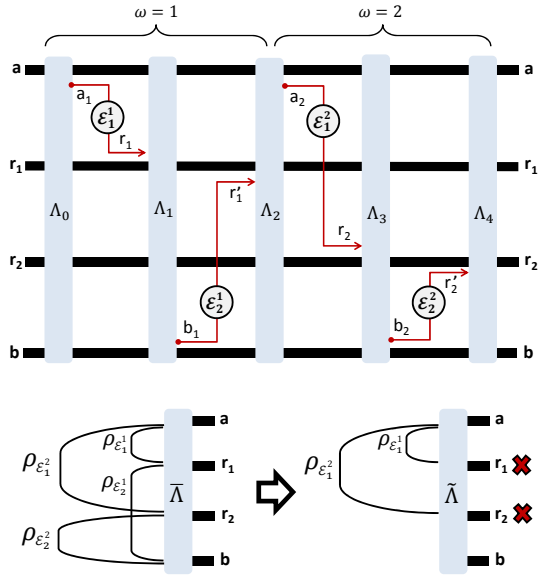

FIG. 8: **Stretching of two routes of a network**. The first transmission through the two routes can be stretched into the output state $\rho_{\mathbf{aRb}} = \bar{\Lambda}(\otimes_{\omega,i}\, \rho_{\mathcal{E}_i^\omega})$, where $\mathbf{R} = \mathbf{r}_1\mathbf{r}_2$ are the middle repeaters. In each route we identify the channel with minimum entanglement flux, here assumed to be $\mathcal{E}_1^1$ and $\mathcal{E}_1^2$. We then keep the corresponding Choi matrices $\rho_{\mathcal{E}_1^1}$ and $\rho_{\mathcal{E}_1^2}$ while the others are included in the LOCC (which remains LO for Alice and Bob). Finally, we trace the middle repeaters.

Corollary 7 *Consider a quantum network whose points are connected by distillable channels (e.g., lossy channels, quantum-limited amplifiers, dephasing or erasure channels). There is an optimal route $\tilde{\omega}$ between the end-points: This is the route with maximum entanglement flux, whose value provides all the network capacities, i.e.,*

$$\mathcal{C}(\mathcal{N}) = \Phi_{\tilde{\omega}} = \max_{\omega} \Phi_\omega = \Phi(\mathcal{N}) \ . \tag{68}$$

Equivalently, we may write

$$\mathcal{C}(\mathcal{N}) = \max_{\omega} \min_{i} \mathcal{C}(\mathcal{E}_i^\omega) \ . \tag{69}$$

Proof. It is sufficient to show that $\Phi_{\tilde{\omega}}$ is an achievable rate. Restricting the routing set to the optimal route $\tilde{\omega}$ and ignoring all the network points not belonging to that route, we have a chain of repeaters between the two end-points for which we may apply previous Corollary 5. The repeater-assisted capacity of the optimal route $\mathcal{C}(\{\mathcal{E}_i^{\tilde{\omega}}\})$ is an achievable bound which satisfies $\mathcal{C}(\{\mathcal{E}_i^{\tilde{\omega}}\}) = \Phi_{\tilde{\omega}} = \min_i \mathcal{C}(\mathcal{E}_i^{\tilde{\omega}})$. Thus, we have $\mathcal{C}(\mathcal{N}) \geq \Phi_{\tilde{\omega}}$ which, combined with Eq. (65), provides Eqs. (68) and (69). ■

Previous Corollary 7 reduces the optimal use of a quantum network to the resolution of a classical max-min problem. Given two points of the network we compute the entanglement flux for each route connecting the two points and then we take the maximum value. This procedure can be applied to very important cases such as bosonic lossy networks or spin networks affected by dephasing or erasure. We may even consider hybrid networks involving both DV and CV systems, such as spin-bosonic networks affected by erasure and loss.

As an example, consider a bosonic network with lossy channels, which well describes both free-space or fibre-based optical communications. Along the route ω, we have a sequence of lossy channels with transmissivities $\{\eta_i^\omega\}$. We then compute the minimum transmissivity $\eta_\omega := \min_i \eta_i^\omega$ which provides the entanglement flux of the route $\Phi_\omega = -\log_2(1-\eta_\omega)$. The network capacity is given by the maximization of Φ_ω over all the routes connecting Alice and Bob. This is equal to

$$\mathcal{C}_{\text{loss}}(\mathcal{N}) = -\log_2(1-\tilde{\eta}), \quad \tilde{\eta} := \max_{\omega} \eta_\omega. \tag{70}$$

Similar conclusions can be derived for Gaussian networks with quantum-limited amplifiers or a mix of amplifiers and lossy channels. Consider a network of amplifiers, where route ω is composed by quantum-limited amplifiers with gains $\{g_i^\omega\}$. We then compute the maximum gain $g_\omega := \max_i g_i^\omega$, providing the entanglement flux of the route $\Phi_\omega = \log_2[g_\omega/(g_\omega - 1)]$. As before, the network capacity is given by maximizing Φ_ω over all the routes between the two end-points, which leads to

$$\mathcal{C}_{\text{amplifier}}(\mathcal{N}) = \log_2[\tilde{g}/(\tilde{g}-1)], \quad \tilde{g} := \min_{\omega} g_\omega. \tag{71}$$

We can also compute the network capacities in spin networks where links are affected by dephasing or erasure or a mix of the two errors. For instance, in a spin network with dephasing, where route ω is composed of an ensemble of dephasing channels with probabilities $\{p_i^\omega\}$, we compute $\Phi_\omega = 1 - H_2(p_\omega)$ where $p_\omega := \max_i p_i^\omega$. Then, we derive the network capacity

$$\mathcal{C}_{\text{dephasing}}(\mathcal{N}) = 1 - H_2(\tilde{p}), \quad \tilde{p} := \min_{\omega} p_\omega. \tag{72}$$

Finally, for a spin network affected by erasures, where route ω is composed by erasure channels with probabilities $\{p_i^\omega\}$, we compute the entanglement flux $\Phi_\omega = 1 - p_\omega$ where $p_\omega := \max_i p_i^\omega$. By optimizing over the routes, we derive the network capacity

$$\mathcal{C}_{\text{erasure}}(\mathcal{N}) = 1 - \tilde{p}, \quad \tilde{p} := \min_{\omega} p_\omega. \tag{73}$$

E. Remarks on the optimal route

Some considerations on the optimal use of a quantum network are in order. First of all, note that there could be multiple solutions that may be constructed from an optimal route by the introduction of loops. For instance, as shown in Fig. 9, from the optimal route $\tilde{\omega}$ we might construct an alternate route ω' having the same entanglement flux $\Phi_{\omega'} = \Phi_{\tilde{\omega}}$, but including extra connections $\{\mathcal{E}_i'\}$ with $\Phi(\mathcal{E}_i') \geq \Phi_{\tilde{\omega}}$. This type of alternate solution can be excluded by restricting Ω to collision-free routes. Clearly this reduction is just a classical procedure.

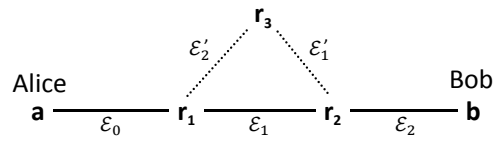

FIG. 9: Possible routes between two end-points. Suppose that Alice and Bob are connected by the optimal route $\tilde{\omega}:\mathbf{a}-\mathbf{r}_1-\mathbf{r}_2-\mathbf{b}$ (solid line), with entanglement flux $\Phi_{\tilde{\omega}}=\Phi(\mathcal{E}_1)$. There may be another route $\omega'\in\Omega$ with $\Phi_{\omega'}=\Phi_{\tilde{\omega}}$, which includes a loop as in the figure, i.e., $\omega':\mathbf{a}-\mathbf{r}_1-\mathbf{r}_2-\mathbf{r}_3-\mathbf{r}_1-\mathbf{r}_2-\mathbf{b}$ (solid and dotted line). In this route the entanglement fluxes of the channels $\mathcal{E}_1'$ and $\mathcal{E}_2'$ are greater than $\Phi_{\tilde{\omega}}$. Such a solution is excluded by reducing Ω to collision-free routes.

Then, note that the network capacity $\mathcal{C}(\mathcal{N})$ provides the maximum number of target bits (secret bits, ebits or qubits) per use of the network or, equivalently, per system routed. In order to reach this optimal rate, the points on the optimal route just need to perform independent two-way adaptive protocols between each pair of nearest-neighbor points i and $i+1$. In particular, such independent protocols can be performed *simultaneously*. If we explicitly introduce a clock, defined as number γ of network uses per second, then $\gamma\mathcal{C}(\mathcal{N})$ provides the maximum number of bits per second.

However, there may be situations, where the previous nearest-neighbor adaptive protocols can only be performed sequentially, which means that the distribution between points i and $i+1$ only starts after the distribution between $i-1$ and i. Such a time constraint may change the optimal solution. As a matter of fact it rescales the effective clock of a route depending on the number of transmissions. For a route with $N+1$ transmissions, we have $\gamma\to\gamma(N+1)^{-1}$. Thus, in this scenario, the optimal route will be that maximizing the re-scaled entanglement flux $\Phi_{\omega}(N+1)^{-1}$.

V. CONCLUSIONS

In this work we have investigated the optimal rate performance of quantum communications in network-like scenarios, considering linear chains of quantum repeaters and, more generally, quantum networks with arbitrary topology. Using the method of teleportation stretching we have shown that the most general adaptive protocols performed in these scenarios can be reduced to an ensemble of Choi matrices followed by a trace-preserving LOCC. This reduction is generally possible for any linear chain or quantum network composed by stretchable channels which suitably commute with teleportation.

In particular, we have computed the repeater-assisted and network-assisted capacities for secret-key generation, entanglement distillation and quantum communication under the most important decoherence models for both continuous- and discrete-variable systems, including loss, amplification, dephasing and erasure. These capacities turn out to have remarkably simple formulas.

The applicability of our results is very wide. As a matter of fact, they establish the ultimate rate for optical/telecom quantum communications in chains of quantum repeaters and bosonic networks which are subject to loss. This rate bounds the optimal performance which is achievable by any end-to-end [16, 17] QKD protocol. Our findings also determine the optimal rate for transmitting quantum information and distilling entanglement in DV scenarios, such as a spin chain or a spin network whose connections are modelled by dephasing or erasure channels. More generally, our results may be applied to completely hybrid scenarios, involving both DV and CV systems, as is expected for the case of a distributed quantum computing architecture or quantum Internet.

In conclusion, by establishing the ultimate performance of network quantum communications with different types of systems and different models of decoherence, our work contributes to understand the best technologies to be used for the next-generation quantum networks. Specifically for quantum repeaters, our results provide the full meter to evaluate their effective performance: We may tell if a design is close to be optimal or not, and how far a technology can be improved towards the realization of high-speed quantum communications.

Acknowledgments. This work has been supported by the EPSRC via the 'UK Quantum Communications HUB' (EP/M013472/1) and 'qDATA' (EP/L011298/1).

Appendix A: Stretching of a chain

Suppose that the jth transmission occurs between repeater $\mathbf{r}_i$ and $\mathbf{r}_{i+1}$ via channel $\mathcal{E}_i$. Let us denote by $\rho^j_{\mathbf{aRb}}$ the total state of the chain after this transmission, where $\mathbf{R}=\mathbf{r}_1\mathbf{r}_2\ldots\mathbf{r}_N$ is the ensemble of all the repeaters. Then, we may modify Eq. (28) into

$$\rho^j_{\mathbf{aRb}}=\bar{\Lambda}_j\left(\rho^{j-1}_{\mathbf{aRb}}\otimes\rho_{\mathcal{E}_i}^{R_iR_{i+1}}\right) \tag{A1}$$

where R_i and R_{i+1} are ancillary systems absorbed by repeaters $\mathbf{r}_i$ and $\mathbf{r}_{i+1}$, respectively, and $\bar{\Lambda}_j$ is a trace-preserving LOCC. Suppose that the transmissions are sequential, as described in the basic repeater protocol, so that the first transmission is between Alice $\mathbf{a}=\mathbf{r}_0$ and the first repeater $\mathbf{r}_1$ and so on. This means to set $j=i+1$ in Eq. (A1) for $i=0,\ldots,N$. Starting from the separable state $\rho^0_{\mathbf{aRb}}=\sigma_{\mathbf{aRb}}$, we derive

$$\rho^1_{\mathbf{aRb}}=\bar{\Lambda}_1\left(\sigma_{\mathbf{aRb}}\otimes\rho_{\mathcal{E}_0}^{R_0R_1}\right) \tag{A2}$$

$$\rho^2_{\mathbf{aRb}}=\bar{\Lambda}_2\left(\rho^1_{\mathbf{aRb}}\otimes\rho_{\mathcal{E}_1}^{R_1R_2}\right) \tag{A3}$$

$$\vdots$$

$$\rho^{N+1}_{\mathbf{aRb}}=\bar{\Lambda}_{N+1}\left(\rho^N_{\mathbf{aRb}}\otimes\rho_{\mathcal{E}_N}^{R_NR_{N+1}}\right), \tag{A4}$$

which leads to

$$\rho^{N+1}_{\mathbf{aRb}}=\bar{\Lambda}_{N+1}\circ\cdots\circ\bar{\Lambda}_1\left(\sigma_{\mathbf{aRb}}\otimes_{i=0}^N\rho_{\mathcal{E}_i}^{R_iR_{i+1}}\right). \tag{A5}$$

This completes the first use of the chain. In the second use of the chain, the input state becomes $\rho_{\mathbf{aRb}}^{N+1}$ and we iterate Eq. (A1) with $j = i + N + 2$, so that we have

$$\rho_{\mathbf{aRb}}^{N+2} = \bar{\Lambda}_{N+2}\left(\rho_{\mathbf{aRb}}^{N+1} \otimes \rho_{\mathcal{E}_0}^{R_0 R_1}\right), \tag{A6}$$

an so on, with similar expressions up to $\rho_{\mathbf{aRb}}^{2N+2}$. By replacing as before, we derive

$$\rho_{\mathbf{aRb}}^{2N+2} = \bar{\Lambda}_{2N+2} \circ \cdots \circ \bar{\Lambda}_1 \left[\sigma_{\mathbf{aRb}} \otimes_{i=0}^{N} \left(\rho_{\mathcal{E}_i}^{R_i R_{i+1}}\right)^{\otimes 2}\right]. \tag{A7}$$

After n uses of the chain, we then get

$$\rho_{\mathbf{aRb}}^{n(N+1)} = \bar{\Lambda}_{n(N+1)} \circ \cdots \circ \bar{\Lambda}_1 \left[\sigma_{\mathbf{aRb}} \otimes_{i=0}^{N} \left(\rho_{\mathcal{E}_i}^{R_i R_{i+1}}\right)^{\otimes n}\right]. \tag{A8}$$

This can be re-written as

$$\rho_{\mathbf{aRb}}^{n(N+1)} := \rho_{\mathbf{aRb}}^{n} = \bar{\Lambda}\left(\otimes_{i=0}^{N} \rho_{\mathcal{E}_i}^{\otimes n}\right), \tag{A9}$$

where we exploit the fact that $\sigma_{\mathbf{aRb}}$ is separable and, therefore, can be included in the global LOCC. Finally, tracing out the repeaters $\mathbf{R}$, we may write

$$\rho_{\mathbf{ab}}^{n} = \bar{\Lambda}_{\mathbf{ab}}\left(\otimes_{i=0}^{N} \rho_{\mathcal{E}_i}^{\otimes n}\right), \tag{A10}$$

where $\bar{\Lambda}_{\mathbf{ab}}$ is another trace-preserving LOCC.

It is important to note that we can equivalently reach the final result of Eq. (A10) also considering other ordering for the transmissions between the repeaters, i.e., not necessarily sequential. One can check that a random permutation of the order of the transmissions corresponds to a permutation of the $\bar{\Lambda}_j$ in Eq. (A8).

[1] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2002).

[2] M. M. Wilde, *Quantum information theory* (Cambridge University Press, Cambridge, 2013).

[3] A. Holevo, *Quantum systems, channels, information: A mathematical introduction* (De Gruyter, Berlin-Boston, 2012).

[4] S. L. Braunstein and P. van Loock, *Quantum information theory with continuous variables*, Rev. Mod. Phys. **77**, 513 (2005).

[5] C. Weedbrook *et al., Gaussian quantum information*, Rev. Mod. Phys. **84**, 621 (2012).

[6] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proc. IEEE International Conf. on Computers, Systems, and Signal Processing, Bangalaore, pp. 175–179 (1984).

[7] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661-663 (1991).

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography*, Rev. Mod. Phys. **74**, 145 (2002).

[9] V. Scarani *et al.*, *The security of practical quantum key distribution*, Rev. Mod. Phys. **81**, 1301 (2009).

[10] C. Elliott, *Building the quantum network*, New J. Phys. **4**, 46 (2002).

[11] M. Peev *et al.*, *The SECOQC quantum key distribution network in Vienna*, New J. Phys. **11**, 075001 (2009).

[12] M. Sasaki *et al.*, *Field test of quantum key distribution in the Tokyo QKD Network*, Optics Express **19**, 10387-10409 (2011).

[13] B. Fröhlich *et al.*, *A quantum access network*, Nature **501**, 69-72 (2013).

[14] K. A. Patel *et al.*, *Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks*, Appl. Phys. Lett. **104**, 051123 (2014).

[15] B. Fröhlich *et al.*, *Quantum secured gigabit optical access networks*, Preprint arXiv:1509.03496 (2015).

[16] J. H. Saltzer, D. P. Reed, and D. D. Clark, *End-to-end arguments in system design*, ACM Transaction on Computer System (TOCS) **2**, 277-288 (1984).

[17] P. Baran, *On distributed communications networks*, IEEE Trans. Commun. Syst. **12**, 1-9 (1964).

[18] S. L. Braunstein and S. Pirandola, *Side-channel-free quantum key distribution*, Phys. Rev. Lett. **108**, 130502 (2012).

[19] S. Pirandola *et al.*, *High-rate measurement-device-independent quantum cryptography*, Nature Photon. **9**, 397-402 (2015).

[20] S. Pirandola *et al.*, *Reply to 'Discrete and continuous variables for measurement-device-independent quantum cryptography'*, Nature Photon. **9**, 773-775 (2015). See also Preprint arXiv.1506.06748 (2015).

[21] L. C. Comandar *et al.*, *Quantum cryptography without detector vulnerabilities using optically-seeded lasers*, Preprint arXiv:1509.08137 (2015).

[22] Y.-L. Tang *et al.*, *Measurement-device-independent quantum key distribution over untrustful metropolitan network*, Preprint arXiv:1509.08389 (2015).

[23] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895-1899 (1993).

[24] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, *Advances in quantum teleportation*, Nature Photon. **9**, 641-652 (2015).

[25] H. J. Kimble, *The Quantum Internet*, Nature **453**, 1023-1030 (2008).

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

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

[28] Note that we use the compact notation $\mathcal{C}$ for the generic two-way assisted capacity. Depending on the specific task, this may represent the secret-key capacity K, the two-way assisted entanglement-distillation capacity D_2, or the two-way assisted quantum capacity Q_2. This notation is adopted not only for a single channel $\mathcal{C}(\mathcal{E})$, but also for a chain of repeaters $\mathcal{C}(\{\mathcal{E}_i\})$, a broadcast channel $\mathcal{C}^k$, and also for a quantum network $\mathcal{C}(\mathcal{N})$. In all cases considered, we have the hierarchy $Q_2 = D_2 \leq K$. Thus, when we write an upper bound $\mathcal{C} \leq \Phi$, we implicitly

mean $Q_2 = D_2 \leq K \leq \Phi$. Then, when we write an equality $\mathcal{C} = \Phi$, we implicitly mean $Q_2 = D_2 = K = \Phi$.

[29] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum repeaters: The role of imperfect local operations in quantum communication*, Phys. Rev. Lett. **81**, 5932-5935 (1998).

[30] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, *Quantum repeaters based on entanglement purification*, Phys. Rev. A **59**, 169 (1999).

[31] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Long-distance quantum communication with atomic ensembles and linear optics*,Nature (London) **414**, 413 (2001).

[32] Z. Zhao, T. Yang, Y.-A. Chen, A.-N. Zhang, and J.-W. Pan, *Experimental Realization of Entanglement Concentration and a Quantum Repeater*, Phys. Rev. Lett. **90**, 207901 (2003).

[33] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, *Quantum Repeaters with Photon Pair Sources and Multimode Memories,* Phys. Rev. Lett. **98**, 190503 (2007).

[34] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J.-W. Pan, *Experimental demonstration of a BDCZ quantum repeater node*, Nature **454**, 1098-1101 (2008).

[35] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, *Quantum Repeaters using Coherent-State Communication*, Phys. Rev. A **78**, 062319 (2008).

[36] R. Alleaume, F. Roueff, E. Diamanti, and N. Lutkenhaus, *Topological optimization of quantum key distribution networks*, New J. Phys. **11**, 075002 (2009).

[37] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, *Quantum repeaters based on atomic ensembles and linear optics*, Rev. Mod. Phys. **83**, 33 (2011).

[38] D. E. Bruschi, T. M. Barlow, M. Razavi, and A. Beige, *Repeat-until-success quantum repeaters,* Phys. Rev. A **90**, 032306 (2014).

[39] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Ultrafast and Fault-Tolerant Quantum Communication across Long Distances*, Phys. Rev. Lett. **112**, 250501 (2014).

[40] K. Azuma, K. Tamaki, and W. J. Munro, *All-photonic intercity quantum key distribution,* Nature Comm. **6**, 10171 (2015).

[41] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, *Overcoming lossy channel bounds using a single quantum repeater node,* Preprint arXiv:1508.02811 (2015).

[42] J. Dias and T. C. Ralph, *Continuous Variable Quantum Repeaters*, Preprint arXiv:1505.03626 (2015).

[43] C. Choi, *Completely Positive Linear Maps on Complex matrices*, Linear Algebra Appl. **10**, 285-290 (1975).

[44] M. A. Nielsen and I. L. Chuang, *Programmable Quantum Gate Arrays*, Phys. Rev. Lett. **79**, 321 (1997).

[45] S. Ishizaka and T. Hiroshima, *Asymptotic Teleportation Scheme as a Universal Programmable Quantum Processor,* Phys. Rev. Lett. **101**, 240501 (2008).

[46] As shown in Ref. [26], the optimal strategy for two-way quantum communication over stretchable channels is to restrict the distribution to the forward or backward channel, depending on which one has the highest capacity.

[47] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, *Secure key from bound entanglement*, Phys. Rev. Lett. **94**, 160502 (2005).

[48] Note that maximally-entangled states are specific types of private states [47].

[49] V. Vedral, *The role of relative entropy in quantum information theory*, Rev. Mod. Phys. **74**, 197 (2002).

[50] B. Schumacher and M. A. Nielsen, *Quantum data processing and error correction*, Phys. Rev. A **54**, 2629 (1996).

[51] S. Lloyd, *Capacity of the noisy quantum channel*, Phys. Rev. A **55,** 1613 (1997).

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

[53] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, *Direct and reverse secret-key capacities of a quantum channel*, Phys. Rev. Lett. **102**, 050503 (2009).

[54] I. Devetak and A. Winter, *A. Relating quantum privacy and quantum coherence: an operational approach*, Phys. Rev. Lett. **93**, 080501 (2004).

[55] M. Takeoka, S. Guha, and M. M. Wilde, *Fundamental rate-loss tradeoff for optical quantum key distribution*, Nature Comms. **5**, 5235 (2014).

[56] L. Banchi, S. L. Braunstein, and S. Pirandola, *Quantum fidelity for arbitrary Gaussian states*, Phys. Rev. Lett. **115**, 260501 (2015).

[57] S. Pirandola, G. Spedalieri, S. L. Braunstein, N. J. Cerf, and S. Lloyd, *Optimality of Gaussian discord*, Phys. Rev. Lett. **113**, 140405 (2014).

[58] S. Pirandola, *Quantum discord as a resource for quantum cryptography*, Sci. Rep. **4**, 6956 (2014).

[59] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, (Wiley, New Jersey, 2006).

[60] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, *Capacities of quantum erasure channels*, Phys. Rev. Lett. **78**, 3217 (1997).

[61] P. Slepian, *Mathematical Foundations of Network Analysis* (Springer-Verlag, New York, 1968).