Rate limits in quantum networks with lossy repeaters

Riccardo Laurenza,[1] Nathan Walk,[1,2] Jens Eisert,[1,3,4] and Stefano Pirandola[5]

[1] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*
[2] *Toshiba Research Europe Limited, 208 Cambridge Science Park, Cambridge CB4 0GZ, United Kingdom*
[3] *Helmholtz-Zentrum Berlin für Materialien und Energie, Hahn-Meitner-Platz 1, 14109 Berlin, Germany*
[4] *Fraunhofer Heinrich Hertz Institute, 10587 Berlin, Germany*
[5] *Department of Computer Science, University of York, York YO10 5GH, United Kingdom*

The derivation of ultimate limits to communication over certain quantum repeater networks have provided extremely valuable benchmarks for assessing near-term quantum communication protocols. However, these bounds are usually derived in the limit of ideal devices and leave questions about the performance of practical implementations unanswered. To address this challenge, we quantify how the presence of loss in repeater stations affect the maximum attainable rates for quantum communication over linear repeater chains and more complex quantum networks. Extending the framework of node splitting, we model the loss introduced at the repeater stations and then prove the corresponding limits. In the linear chain scenario we show that, by increasing the number of repeater stations, the maximum rate cannot overcome a quantity which solely depends on the loss of a single station. We introduce a way of adapting the standard machinery for obtaining bounds to this realistic scenario. The difference is that whilst ultimate limits for any strategy can be derived given a fixed channel, when the repeaters introduce additional decoherence, then the effective overall channel is itself a function of the chosen repeater strategy. Classes of repeater strategies can be analysed using additional modelling and the subsequent bounds can be interpreted as the optimal rate within that class.

I. INTRODUCTION

Quantum communication is one of the most practically relevant applications of the quantum technologies, offering the perspective of secure communication based on physical laws [1–9]. While security can be proven to hold under enormously generous and general conditions, it can only be guaranteed for sufficiently low levels of loss. For short distances, this does not constitute a technological challenge. However, for large distances, secure quantum communication becomes very challenging, since all loss has to be attributed to an eavesdropper and this prevents achieving arbitrarily high rates of secure bits. Similar limitations arise for the maximum attainable rates for quantum information (qubits) transmission entanglement (ebits) distribution over lossy bosonic channels that conveniently describe optical fibres or free-space links. More specifically, it has been established that, for any point-to-point transmission protocol over a lossy bosonic channel with transmissivity equal to $\eta \in (0,1)$, allowing the two parties to exploit unlimited two-way classical communications, the maximum achievable rates for key generation, entanglement distribution, and quantum bit transmissions, are all equal to the *repeaterless PLOB bound* $-\log_2(1-\eta)$ [10].

This severe limitation of direct point-to-point transmission is not a road block, however. Intermediate stations, referred to as *quantum repeaters* [11], can overcome this limitation and, in principle, allow communication over arbitrary distances. Since the appearance of the first quantum repeater proposal [12], the goal of extending the distance at which two parties can faithfully share a secret key or entanglement has stimulated a plethora of repeater-assisted quantum communication schemes. From the conceptual point of view, a quantum repeater is a scheme in which entanglement is first distributed to intermediate nodes. Then, the quality is improved by means of entanglement distillation, transforming a collection of weakly entangled states into a smaller number of more highly entangled states. In the final step, one performs sequential entanglement swapping, bringing quantum systems together that have no joint past, to entangle the anticipated nodes. The difficulty of assessing precise rates of (quantum) information transmission and specifically of key rates gives rise to the necessity to identify bounds that are agnostic to the specific implementation chosen. Only in such a realm, can ultimate bounds for quantum communication be established. Along this line of thought, a fundamental result about the rates at which two end-nodes in a linear repeater chain can transmit quantum information, distribute entanglement, or generate a secret key has been established in Ref. [13]. In particular, when two users, say Alice and Bob, are connected by a line of $N-1$ middle repeater nodes, linked together through N optical lossy fibres, the quantum/private capacity of the linear repeater chain, i.e., the ultimate rate for repeater-assisted quantum or private communication between the two end-users is given by [13, Eq. (9)]

$$C(\eta, N) = -\log_2(1 - \sqrt[N]{\eta}) \,, \tag{1}$$

where $\eta > 0$ is the total Alice-to-Bob fibre transmissivity. This expression is derived by exploiting a combination of tools that we briefly recall in the appendices.

It is important to stress that, for a fixed total transmissivity η but large number of repeaters, the end-to-end capacity $C(\eta, N)$ diverges as $\log_2 N$. This feature is immediately connected to the fact that the repeaters are assumed to be ideal, i.e., lossless. Under a more realistic point of view each repeater in the linear repeater chain must be characterised by imperfect components which introduce noise and decoherence to the stored and transmitted quantum states. For instance these internal losses could be the effect of non-unit detection efficiencies, channel-memory coupling losses, memory loading and readout efficiencies. Furthermore, detrimental effects can be introduced by the quantum memories at the nodes while the quantum systems are stored before the on-demand retrieval.

Here, we explicitly account for this crucial aspect and we consequently derive the end-to-end repeater capacity of a lossy bosonic quantum network where the repeater stations are also affected by internal loss. Although loss is not the only source of decoherence, it is often the dominant factor and is an excellent first approximation for an optical fibre channel. Furthermore, using lossy channels as a model for imperfections within the repeater nodes will facilitate derivation of exact formulae for the various capacities of interest.

Our derivation is carried out for the various types of *routing* (single- and multi-path). Our bound hence captures rather general classes of repeater schemes and can be seen as an analog of the repeater-less PLOB in the presence of lossy repeater stations. Given a fixed amount of loss for each repeater node we can immediately evaluate our bounds as a function of transmission losses. However, in real implementations the loss in each node is itself typically a function of the transmission losses. The paradigmatic example is the loss induced by a quantum memory where the necessary storage time usually increases with transmission loss.

To exemplify these findings, we show that, considering a realistic time-dependent model of decoherence for a single repeater station, the achievable rates not only beat the benchmark of the repeater-less PLOB bound, but they are also not that far from the upper limit provided by our revised lossy-repeater capacity. As an example we consider polarisation-based BB84 key distribution protocol over a single repeater node using a simple entanglement swapping protocol with Rubidium memories and show it scales as one quarter of the optimal possible rate for such schemes. Finally, recent years have enjoyed considerable interest in identifying practical schemes for routing in multi-partite *quantum networks* [13–19]. Our results are general enough to accommodate such situations, as we show.

II. NODE SPLITTING

Let us consider a linear sequence $\{s_0, \ldots, s_N\}$ of $N-1$ repeater nodes, where Alice and Bob, the two end stations, are identified with s_0 and s_N, respectively. We assume that each station s_i in the chain is connected to s_{i+1} through an optical fibre described by a Gaussian lossy channel [20] $\mathcal{L}_i$ with transmissivity η_i, for $i = 0, \ldots, N$. Thus, the total transmissivity of the link (e.g., an optical fibre providing the communication channel) connecting Alice and Bob is $\eta = \prod_i \eta_i$. Each node s_i has internal losses that can be quantified by a global transmissivity $\tau_i \in [0, 1]$ obtained by the product of single inefficiencies. In this way we can describe the effect of the node on the incoming quantum systems as another Gaussian lossy channel, mathematically described as a beam splitter mixing the input system with an environment in the vacuum

$$\hat{x}_{\text{out}} = \sqrt{\tau_i}\hat{x}_{\text{in}} + \sqrt{1-\tau_i}\hat{x}_{\text{vac}} \, . \qquad (2)$$

We can further distinguish two different contributions in τ_i: a *transmitting* efficiency τ_i^t, and a *receiving* efficiency τ_i^r. The former is associated for instance with the overall effects of a source efficiency (e.g. photon creation efficiency), a memory read-out efficiency and a memory-channel interface efficiency. The latter involves a detector efficiency, a memory write-in efficiency and channel-memory coupling efficiency in some fashion.

To account for the internal lossy features in the various stations, we perform the *node splitting* depicted in Fig. 1. We split the generic node s_i into three "children" nodes s_i^k ($k = 1, 2, 3$), which are then linked together through a composition of two lossy channels $\mathcal{R}^t_{s_i^2 \to s_i^3}$ and $\mathcal{R}^r_{s_i^1 \to s_i^2}$, with associated transmissivities $\tau_i^{t,r}$. Combining these internal channels with $\mathcal{L}_i$ associated to the ith link, we can model the linear network with noisy quantum repeaters as a sequence of composite quantum channels. More precisely, we can identify a building-block channel, so that the linear network can be described as the collection $\{\mathfrak{C}_i\}_i$ of the following composite quantum channels (see Fig. 1)

$$\mathfrak{C}_i = \mathcal{R}^r_{s^1_{i+1} \to s^2_{i+1}} \circ \mathcal{L}_{i+1} \circ \mathcal{R}^t_{s^2_i \to s^3_i}, \qquad (3)$$

for $i = 1, \ldots, N-1$, while for the two end-nodes we set $\mathcal{R}^r_{s_0^1 \to s_0^2} = \mathcal{R}^t_{s_N^2 \to s_N^3} = \mathcal{I}$, where $\mathcal{I}$ is the identity channel. To simplify notation, we rename $\mathcal{R}^{r,t}_{s_i^k \to s_i^{k+1}} = \mathcal{R}_i^{r,t}$.

By means of the decomposition in Eq. (3), we are able to apply the machinery developed in Ref. [13] to our scenario so we can derive a single-letter upper bound on the secret-key capacity (and therefore on the two-way quantum capacity) of the lossy-repeater linear chain. By performing an entanglement cut labelled by i, we disconnect the chain along the channel $\mathcal{L}_i$. In doing so, we create a bipartition (A, B) of the chain, with $A = \{s_0^1, s_0^2, s_0^3 \ldots, s_i^1, s_i^2, s_i^3\}$ and $B = \{s_{i+1}^1, s_{i+1}^2, s_{i+1}^3 \ldots, s_N^1, s_N^2, s_N^3\}$. This leads us to formulate the following.

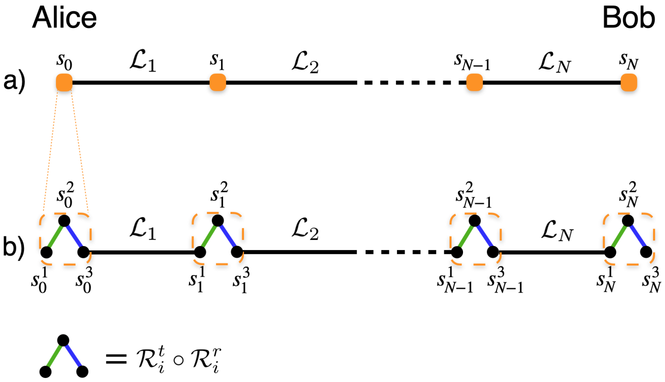

FIG. 1: Node splitting in a repeater chain. a) $N-1$ repeater stations s_i are linked together to form a linear network (chain) between s_0 (Alice) and s_N (Bob). The end-to-end transmissivity is $\eta = \eta_1\eta_2 \cdots \eta_N$, where $\eta_i > 0$ is the transmissivity of the single link described by the quantum lossy channel $\mathcal{L}_i$. b) Node splitting of the linear network. Each node s_i is split into three children nodes $\{s_i^1, s_i^2, s_i^3\}$ and two links $s_i^1 - s_i^2$, $s_i^2 - s_i^3$ are added. The overall effect of the internal losses in the i-th node is then described by the composition $\mathcal{R}_i^t \circ \mathcal{R}_i^r$ of two additional quantum lossy channels.

Definition 1 (Lossy repeaters) *The state shared by Alice and Bob at the output of the most general adaptive protocol over n uses of the repeater chain is given by*

$$\rho^n_{a,b} = \Lambda_i \left(\sigma^{\otimes n}_{\mathfrak{C}_i}\right) , \tag{4}$$

where Λ_i is a trace-preserving local operation with classical communication *(LOCC) while $\sigma_{\mathfrak{C}_i}$ is the Choi matrix of the channel $\mathfrak{C}_i$, which is defined as $\sigma_{\mathfrak{C}_i} := (\mathcal{I} \otimes \mathfrak{C}_i)(\Phi)$.*

Here, $\mathcal{I}$ is the identity channel and Φ is a maximally-entangled state. More precisely, the above equation has to be intended as asymptotic, since for CV systems, the maximally entangled state is asymptotic and as a consequence the Choi matrix $\sigma_{\mathfrak{C}_i}$ is obtained as a limit. In the appendix, we give details on this argument. We notice that for $i = 0$ and for $i \geq 1$, the quantum channel $\mathfrak{C}_i$ is a pure loss channel or a composition of two pure-loss channels respectively. Thus we can conclude that for any $i \geq 0$, $\mathfrak{C}_i$ is a distillable channel, for which the two-way quantum and private capacities are identical and exactly determined, i.e. [10]

$$\mathcal{C}(\mathfrak{C}_i) = E_R(\sigma_{\mathfrak{C}_i}) = D_1(\sigma_{\mathfrak{C}_i}) , \tag{5}$$

where $E_R(\sigma_{\mathfrak{C}_i})$ is the *relative entropy of entanglement* of the Choi matrix $\sigma_{\mathfrak{C}_i}$ and $D_1(\sigma_{\mathfrak{C}_i})$ is the entanglement that can be *distilled* from the Choi matrix with one-way, forward or backward, classical communication (see the appendix for a recap about these types of capacities).

By exploiting Theorem 7 in Ref. [13], we conclude that the two-way quantum/private capacity of the linear chain with lossy repeaters satisfies

$$\mathcal{C}(\{\mathfrak{C}_i\}) = \min_{0\leq i\leq N} E_R(\sigma_{\mathfrak{C}_i}) = \min_{0\leq i\leq N} \mathcal{C}(\mathfrak{C}_i). \tag{6}$$

Using the PLOB bound and the fact that the transmissivity of a composition of lossy channels is given by the product of the individual transmissivities, we can state the following theorem which generalizes the formula for ideal repeaters given in Ref. [13],

Theorem 1 (Lossy-repeater capacity) *The ultimate achievable rate for repeater-assisted quantum/private communication between the two-end users of a linear network with $N-1$ lossy quantum repeaters connected by N pure-loss channels is given by*

$$\mathcal{C}(\{\mathfrak{C}_i\}) = \min_i [-\log_2(1 - \tau^t_i \tau^r_{i+1} \eta_{i+1})] , \tag{7}$$

i.e., it equals the minimum capacity of the channel $\mathfrak{C}_{\rm i}$ describing the loss of node i, the pure loss channel $i+1$ and the loss of node $i+1$.

Let us assume that the end-users, Alice and Bob, are at a distance L apart and connected by an optical fibre whose transmissivity η decays exponentially as $\eta = e^{-\alpha L}$ (typically, $\alpha = 0.2$dB/km). If $N-1$ lossy repeaters are inserted along the line, the optimal configuration is represented by equally spaced nodes at a distance $L_0 = L/N$, so we have $\eta_i = \sqrt[N]{\eta}$ for each i. We can thus recast Eq. (7) as follows

$$\mathcal{C}(\{\mathfrak{C}_i\}) = -\log_2(1 - \widetilde{\tau} \sqrt[N]{\eta})] , \tag{8}$$

where we have defined $\widetilde{\tau} := \min_{i\geq 0} \tau^r_i \tau^t_{i+1}$. For simplicitly, assume that all the nodes are built and equipped with the same components, i.e., $\tau^r_i = \tau^r$ and $\tau^t_i = \tau^t$, for all $i \in [0, N]$. We then get

$$\mathcal{C}(\{\mathfrak{C}_i\}) \to C_\tau(\eta, N) = -\log_2(1 - \tau \sqrt[N]{\eta}) , \tag{9}$$

where $\tau := \tau^r \tau^t$. If we now consider a large number of nodes we obtain the following expansion

$$C_\tau(\eta, N \gg 1) \simeq -\log_2(1-\tau) + \frac{\tau \log_2 \eta}{(1-\tau)N} . \tag{10}$$

We can thus see that, by increasing the number of repeaters between Alice and Bob, i.e., by taking the limit of $N \to \infty$, the lossy-repeater capacity is bounded by the quantity $-\log_2(1-\tau)$ that depends solely on the loss within a node. In other words, even if we are allowed to arbitrarily increase the number of repeaters on the line, the optimal rate will be anyway bounded by the inevitable internal loss which act as ultimate bottleneck in the process.

III. TIME-DEPENDENCE AND REALISTIC REPEATER PROTOCOLS ON A QUANTUM LINEAR NETWORK

While the above results illuminate the performance of repeater networks with imperfect devices, there is a certain tension between our desire to quantify the ultimate limits to communication whilst also providing formulae that are as relevant as possible to near term demonstrations. The reason for this is that the bounds derived above, whilst totally general in the sense of applying to an optimal two-way LOCC encoding and decoding strategies, only hold for a given channel. However, the effective channel induced by the decoherence of realistic repeater nodes is itself, to some extent, determined by the choice of repeater protocol. For example, the effective loss experienced by a system stored in a quantum memory is a function of the ratio between memory coherence time and the required storage time, but this latter quantity can change depending upon the chosen protocol. In this section, we address this issue by taking into account the role played by time. Incorporating these effects is crucial to obtain tighter bounds that provide more accurate benchmarks for realistic repeater protocols with imperfect devices. This is also a powerful example of how our relatively simple model can be used to meaningfully compare different protocols, as the major differences between them often boil down to variations in timing.

Ultimately, some of the operations involved in the design of repeater-assisted quantum communication and entanglement distribution protocols are intrinsically probabilistic. In memory-based quantum repeater protocols, such fundamental operations are represented by heralded entanglement generation (and possibly distillation) between neighbouring nodes and swapping that transfers such entanglement to nodes at increasing distance. Thus, besides the time required for the transmission of the quantum information carriers and classical heralding signals, which is limited by the speed of light, a finite time is also needed while waiting for success of various operations at the different repeater stations.

As a good first order approximation we can model the memories as time-dependent lossy channels with transmission given by (see, e.g., Ref. [21]),

$$\tau_{\mathrm{mem}}(t) = \tau_0 e^{-t/t_c} \ . \tag{11}$$

where τ_0 is the maximum memory efficiency and t_c is the the coherence time.

The key task remaining to evaluate these bounds is to correctly model the expected storage time. Fortunately, this problem has been well studied in the literature [22, 23]. The situation can be analysed abstractly by defining the success probability of operations on one half of the repeater, p. The expected waiting time will be of the form MT_0, where $T_0 > 0$ is the time taken for one attempt and M is the expected number of attempts. As a first illustration, consider the simplest, canonical setup of a linear chain with one repeater station and two segments separated by a total distance, d.

The quantities T_0 and p are both influenced by the choice of repeater protocol. The minimal time unit, T_0, depends upon whether the central station is operating in a *node-receives-photons* (NRP) or a *node-sends-photons* (NSP) configuration [24]. In the former case, T_0 is simply set by R, the clock speed of either the source or the local processing (e.g. memory write-in time), whichever is slower. Thus, $T_0^{\mathrm{NRP}} = 1/R$. In the NSP case, for sufficiently large distances, T_0 will instead be limited by the time taken to transmit quantum states from the central node the end stations and subsequently receive a classical signal heralding their successful arrival and initiating the swap. This corresponds to the time to transmit twice over one segment such that $T_0^{\mathrm{NSP}} = \max\{1/R, d/c\}$. A final subtlety is that in the NSP configuration, even if the first attempt is successful, a state must still be stored at the central for the time taken for at least one quantum transmission and one classical signal heralding success, i.e., a total of $M+2$ time steps.

The probabilistic elements that go into determining p depend upon whether we think of a *continuous variable* (CV) or *discrete variable* (DV) scheme utilising single photon detection. In a DV scheme entanglement distillation can be avoided if desired and all that is strictly necessary is to store single photon until another has arrived that can be used to swap entanglement. Indeed it is this strategy that is currently pursued in state-of-the-art experiments [25, 26] In this scenario, the probabilistic element is then simply the detection probability of a photon across a single link in the repeater chain and

$$p = \sqrt{\eta}\tau^{t,\mathrm{eff}} \tag{12}$$

for a transmission node and an analogous expression for a receiving node. Here $\tau^{t,\mathrm{eff}}$ represents the efficiency of all of the elements in the transmitting nodes except the memory. These quantities, such as write-in, read-out or or detection efficiencies, will all be time independent and can be captured by single constant. Note that certain nodes in a chain may not have memories.

In the CV case, the arrival of quantum information is deterministic, and the probabilistic element is the entanglement distillation operation. Once distillation has been successfully carried out on either input, that mode is stored until the mode on the other side as also been distilled and then entanglement is swapped. Again, whilst some distillation is essential, the exact amount is a free parameter leading to a trade-off between the success probability and amount of entanglement in the final state. There are only a relatively small number of CV repeater protocols [27–30] with arguably the most mature being those based upon a so-called *noiseless linear amplifier* (NLA) [31, 32]. The NLA acts with a gain g, and the success probability can be upper bounded by $p \leq 1/g^2$, although this bound can be very loose in some circumstances [33]. This is in principle a free parameter, but a reasonable strategy would be to adjust the gain to reverse the effects of the expected losses prior to distillation. To undo a lossy channel of transmission τ requires a gain of $g^2 = 1/\tau$. For these choices, a CV distillation would have success probability upper bounded by (12), exactly as for a DV scheme.

Putting all of this together, we compute the expected value of the memory transmission for the NRP and NSP configurations as [22, 23],

$$\begin{aligned}
\bar{\tau}_{\mathrm{mem}}^{\mathrm{NRP}} &= \mathbb{E}\left(\tau_0 e^{MT_0/t_c}\right), \\
&= \frac{p}{2-p}\left(\frac{2}{1-e^{-T_0^{\mathrm{NRP}/t_c}}(1-p)} - 1\right), \\
\bar{\tau}_{\mathrm{mem}}^{\mathrm{NSP}} &= \mathbb{E}\left(\tau_0 e^{(M+2)T_0/t_c}\right) \\
&= \frac{p}{2-p}\left(\frac{e^{-\frac{2T_0^{\mathrm{NSP}}}{t_c}}\left((1-p)+e^{T_0^{\mathrm{NSP}}/t_c}\right)}{e^{T_0^{\mathrm{NSP}}/t_c}-(1-p)}\right).
\end{aligned} \tag{13}$$

In either the NRP or NSP protocol, the total loss over one link will include whatever constant detection or coupling efficiencies are present along with the additional lossy channel induced by the memory, which will be at either the receiving or transmitting nodes. This means in either case we could write the total repeater losses as $\tau_i^t \tau_{i+1}^r = \tau_i^{t,\mathrm{eff}} \tau_{i+1}^{r,\mathrm{eff}} \tau_{\mathrm{mem}}$. Thus we can substitute (13) into (7) and, using parameters from Ref. [24], evaluate the bounds for some representative repeater platforms. We present the results for a platform based on Rubidium memories in Fig. 2. Note that because we are explicitly considering time in our analysis we are able to calculate rates in terms of bits per second, which is the quantity that is ultimately important for applications, as opposed to the more common bits per channel use.

Crucially, we see that our upper bound now has the same qualitative shape as a real repeater implementation. For short distances, where the storage times are small relative to the memory coherence time, the key rate scales as an ideal repeater with an offset due to extra losses at the station. However, for larger distances, the necessary storage time becomes comparable to the memory coherence time and thus the effective loss falls off exponentially faster. In this situation, the

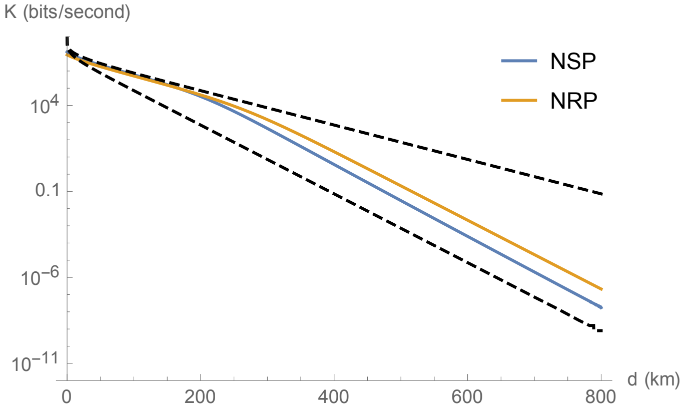

FIG. 2: Upper bounds to the secret key rate for both NSP and NRP protocols using Rubidium memories taken from Ref. [24]. Parameters are: total efficiencies (which is what Ref. [24] refers to as P_{link}) of $(\tau^{\text{eff}})^2 = 0.7$, a coherence time of 100 milliseconds and clock speed of $R = 5{\times}10^6$. The lower and the upper dashed black lines are respectively the repeaterless PLOB bound [10] and the one-station repeater-assisted capacity [13].

protocol fails to follow the ideal repeater scaling, regressing to scale similarly to the repeaterless bound. For certain system parameters our upper bounds can even drop below the repeaterless scaling as the waiting times for the NSP protocol cause additional losses that destroy any benefit for a repeater station.

Finally, we can also use our bounds to benchmark specific protocols carried out with the same system parameters. In Fig. 3, we plot the ratio of a BB84 key rate using an entanglement swapping repeater protocol (see Appendix) to our lossy-repeater capacity given in Eq. (7). From this we can conclude that, over lossy repeater networks, standard BB84 and an entanglement swapping repeater is quite close to the optimal protocol, scaling identically for large distances and achieving slightly worse than one quarter of the optimal key rate.

IV. EXTENSION TO GENERAL QUANTUM NETWORKS

Here, we extend the previous analysis from a linear to a more complex quantum network featuring an arbitrary topology, where the two end users aim at sharing entanglement or secret keys through single or multi-path routing strategies.

A. Preliminaries

A *quantum communication network* $\mathbf{N}$ involving N nodes that can be interpreted as entities pursuing quantum communication can be described as an undirected graph $G = (V, E)$, where V is the set of vertices or nodes ($|V| = N$), and E the set of edges linking the elements in V. The set E is determined by the underlying network infrastructure, i.e., an edge

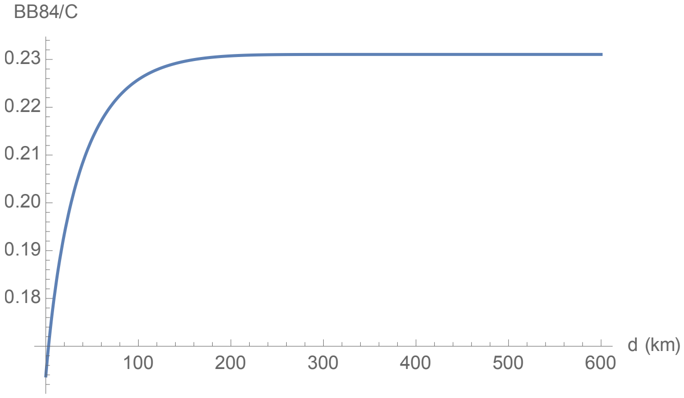

FIG. 3: Ratio of the secret key rate for an BB84 protocol using Rubidium memories taken from Ref. [24] with the lossy-repeater capacity of Eq. (7). Parameters as per Fig. 2.

(ν_i, ν_j) is an element of E if there is a communication channel connecting the two vertices ν_i and ν_j. In a quantum communication scenario the nodes are linked together through a quantum channel $\mathcal{E}_{\nu_i - \nu_j}$. The transmission of quantum information through the quantum channel can be either forward $\nu_i \to \nu_j$ or backward $\nu_j \to \nu_i$. In what follows, we assign an orientation to the network so the quantum systems are always transmitted from sender ν_0 to receiver ν_N. This is a basic formalization of what is commonly called a quantum network.

Quantum information and entanglement can be transmitted and distributed along the network through a generic route R between the two end-users, which is determined by the sequence of vertices $R = \nu_0 - \cdots - \nu_i - \cdots - \nu_N$. In a single network $\mathbf{N}$, the different routes form a set $\mathbf{R_N} = \{R_1, R_2, \ldots\}$. For each route there is an associated sequence of quantum channels, those involved in the routing process. As an example, in panel $a)$ of Fig. 4, we show a fully-connected graph of four vertices that represents a diamond network. The set of all the possible routes from ν_0 to ν_3 is given by $\mathbf{R}_\diamond = \{R_1 = \nu_0 - \nu_1 - \nu_3, R_2 = \nu_0 - \nu_2 - \nu_3, R_3 = \nu_0 - \nu_1 - \nu_2 - \nu_3, R_4 = \nu_0 - \nu_2 - \nu_1 - \nu_3\}$.

B. Node-splitting in the network

As we have done for the linear network, in order to account for a loss model for the stations, we proceed by splitting the nodes ν_i of the network and by inserting two quantum channels $\mathcal{E}_{\nu_i^1 - \nu_i^2}$ and $\mathcal{E}_{\nu_i^2 - \nu_i^3}$, connecting the three children nodes $\{\nu_i^1, \nu_i^2, \nu_i^3\}$. By doing so, the original network $\mathbf{N}$, described by the graph G, is mapped into $\mathbf{N}'$ whose associated new graph is given by $G' = (V', E')$, where $|V'| = 3N$. The generic route R of the ideal repeater network is updated to the route $R' = \overset{\frown}{\nu_0} - \cdots - \overset{\frown}{\nu_i} - \cdots - \overset{\frown}{\nu_N}$, where we have defined the node internal route $\overset{\frown}{\nu_i} := \nu_i^1 - \nu_i^2 - \nu_i^3$. In panel $b)$ of Fig. 4 we show the node-splitting for the diamond network.

It is important to note that, any edge belonging to two dif-

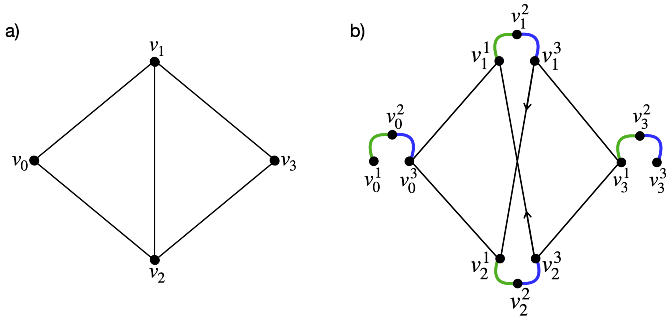

FIG. 4: A diamond network $\mathbf{N}$ of ideal nodes (a) is mapped into a network $\mathbf{N}'$ of lossy nodes (b) by means of splitting. Node ν_i is split in three children $\{\nu_i^1, \nu_i^2, \nu_i^3\}$ which are linked by additional edges (ν_i^1, ν_i^2) and (ν_i^2, ν_i^3) with associated lossy channels $\mathcal{E}_{\nu_i^1-\nu_i^2}$ and $\mathcal{E}_{\nu_i^2-\nu_i^3}$. The undirected link $(\nu_1, \nu_2) \in E$ in $\mathbf{N}$ is replaced, in $\mathbf{N}'$, by two oriented links $\{(\nu_1^3, \nu_2^1), (\nu_2^3, \nu_1^1)\} \in E'$. Accordingly, via the node-splitting, the route set $\mathbf{R}_\diamond$ is mapped into the route set $\mathbf{R}'_\diamond$.

ferent routes with two opposite orientations, must be replaced by two distinct edges through node-splitting. More specifically, in the diamond network scenario of Fig. 4 by observing the route set $\mathbf{R}_\diamond$, the link connecting nodes ν_1 and ν_2 has two opposite orientation in route R_3 and route R_4. This means that, after node-splitting $\mathbf{N} \to \mathbf{N}'$, the edge (ν_1, ν_2) is replaced by two edges (ν_1^3, ν_2^1) and (ν_2^3, ν_1^1) with opposite orientations and the same associated quantum channel, i.e. $\mathcal{E}_{\nu_1^3-\nu_2^1} = \mathcal{E}_{\nu_2^3-\nu_1^1}$. These two links belong to the two distinct routes R'_3 and R'_4 of the new route set $\mathbf{R}'_\diamond := \{R'_1 = \overset{\curvearrowright}{\nu_0} - \overset{\curvearrowright}{\nu_1} - \overset{\curvearrowright}{\nu_3}, R'_2 = \overset{\curvearrowright}{\nu_0} - \overset{\curvearrowright}{\nu_2} - \overset{\curvearrowright}{\nu_3}, R'_3 = \overset{\curvearrowright}{\nu_0} - \overset{\curvearrowright}{\nu_1} - \overset{\curvearrowright}{\nu_2} - \overset{\curvearrowright}{\nu_3}, R'_4 = \overset{\curvearrowright}{\nu_0} - \overset{\curvearrowright}{\nu_2} - \overset{\curvearrowright}{\nu_1} - \overset{\curvearrowright}{\nu_3}\}$.

C. Cuts of the lossy-repeater network

An essential ingredient for our derivation is represented by the entanglement cut of the quantum network [13]. Given the two end-nodes of a network of lossy repeaters, $\overset{\curvearrowright}{\nu_0}$ and $\overset{\curvearrowright}{\nu_N}$ (where $\overset{\curvearrowright}{\nu_i} := \{\nu_i^1, \nu_i^2, \nu_i^3\}$), such an entanglement cut C is defined as a bipartition (V_A, V_B) of the set of nodes of the network such that $\overset{\curvearrowright}{\nu_0}$ belongs to V_A and $\overset{\curvearrowright}{\nu_N}$ belongs to V_B, with the elements of V_A disconnected from the elements of V_B. The entanglement cut induces the definition of the associated cut set K which is the set of the links disconnected by the cut C. In Fig. 5, we show two possible entanglement cuts of the diamond network in the presence of lossy repeater nodes. While the cut C is always performed over the network link of the kind (ν_i^3, ν_j^1) between two distinct nodes i and j, in the cut set K, we include also the internal repeater links which have vertices in common with the link disconnected by C. In other words, if (ν_i^3, ν_j^1) is a network link cut by C, the overall link $(\overset{\curvearrowright}{\nu_i}, \overset{\curvearrowright}{\nu_j}) := (\nu_i^2, \nu_j^2) = (\nu_i^2, \nu_i^3) \cup (\nu_i^3, \nu_j^1) \cup (\nu_j^1, \nu_j^2)$ is an element of the cut set K, i.e. $K = \{(\overset{\curvearrowright}{\nu_i}, \overset{\curvearrowright}{\nu_j}) | , \overset{\curvearrowright}{\nu_i} \in V_A, \overset{\curvearrowright}{\nu_j} \in V_B\}$.

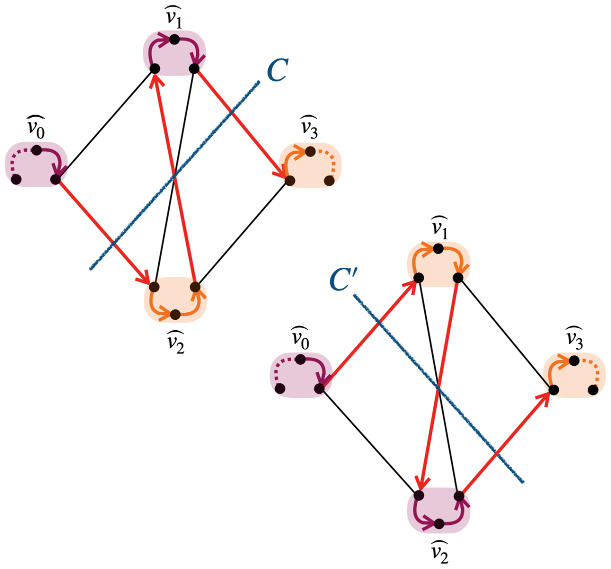
$\overset{\curvearrowright}{\nu_1}$
C
$\overset{\curvearrowright}{\nu_0}$
$\overset{\curvearrowright}{\nu_3}$
$\overset{\curvearrowright}{\nu_2}$
$\overset{\curvearrowright}{\nu_1}$
C'
$\overset{\curvearrowright}{\nu_0}$
$\overset{\curvearrowright}{\nu_3}$
$\overset{\curvearrowright}{\nu_2}$

FIG. 5: Two examples of entanglement cut in a quantum diamond network of lossy nodes. The set of vertices E' of the network is divided into the two bipartitions (V_A, V_B) and (V'_A, V'_B) by the cuts C and C' respectively. In the top network, $V_A = \{\overset{\curvearrowright}{\nu_0}, \overset{\curvearrowright}{\nu_1}\}$ (purple), while $V_B = \{\overset{\curvearrowright}{\nu_2}, \overset{\curvearrowright}{\nu_3}\}$ (orange). In the bottom network, $V'_A = \{\overset{\curvearrowright}{\nu_0}, \overset{\curvearrowright}{\nu_2}\}$ (purple), while $V'_B = \{\overset{\curvearrowright}{\nu_1}, \overset{\curvearrowright}{\nu_3}\}$ (orange). The induced cut sets (thick colored arrows) are respectively given by $K = \{(\overset{\curvearrowright}{\nu_0}, \overset{\curvearrowright}{\nu_2}), (\overset{\curvearrowright}{\nu_2}, \overset{\curvearrowright}{\nu_1}), (\overset{\curvearrowright}{\nu_1}, \overset{\curvearrowright}{\nu_3}\}$ and $K' = \{(\overset{\curvearrowright}{\nu_0}, \overset{\curvearrowright}{\nu_1}), (\overset{\curvearrowright}{\nu_1}, \overset{\curvearrowright}{\nu_2}), (\overset{\curvearrowright}{\nu_2}, \overset{\curvearrowright}{\nu_3}\}$.

Accordingly, the quantum channel associated to the generic element of the cut set is given by

$$\mathfrak{E}_{i,j} := \mathcal{E}_{\nu_j^1-\nu_j^2} \circ \mathcal{E}_{\nu_i^3-\nu_j^1} \circ \mathcal{E}_{\nu_i^2-\nu_i^3} \, , \tag{14}$$

and we set $\mathcal{E}_{\nu_0^1-\nu_0^2} = \mathcal{E}_{\nu_N^2-\nu_N^3} = \mathcal{I}$ for the two end nodes (see the dashed links in Fig. 5).

D. Single-path capacity of the lossy-repeater network

Now that we have obtained a formalisation of the entanglement cuts for a lossy-repeater network (accounting for the node splitting), we are able to derive a corresponding formula for the single-path routing capacity. As per linear networks, our derivation is based on a straightforward generalisation of the ideal scenario with fully error-corrected repeaters. We know from Ref. [13, Th. 6 and 7] that the single-path capacity of a quantum network $\mathbf{N}$ of ideal-repeaters is bounded as follows

$$\mathcal{C}(\mathbf{N}) \leq \min_C E_R(C), \tag{15}$$

where the right hand side term represents the minimization over all the possible cuts of the network of the single-path REE $E_R(C)$ associated to cut C. The latter quantity is defined by maximizing the REE over the edges of the cut set K, i.e.,

$$E_R(C) := \max_{(\nu_i, \nu_j) \in K} E_R(\rho_{\mathfrak{E}_{i,j}}), \tag{16}$$

where $\rho_{\mathcal{E}_{i,j}}$ is the Choi matrix of the lossy channel associated to the link (ν_i, ν_j) (more technically this state and the associated REE are implicitly defined via asymptotic limits [10]).

In contrast, a lower bound can be derived by finding the widest path in the quantum network [13], so we can write

$$\mathcal{C}(\mathbf{N}) \geq C(R^\star) = \min_C \mathcal{C}(C) \tag{17}$$

where $R^\star$ is the optimal route such that the capacity of a single route $\mathcal{C}(R) := \min_\alpha \mathcal{C}(\mathcal{E}_\alpha^R)$ is maximum. Here α is the index over the route and we are implicitly defining $\mathcal{E}_\alpha^R := \mathcal{E}_{\nu_i - \nu_j}$, with edge $(\nu_i, \nu_j) \in R$. Similarly, $\mathcal{C}(C) := \max_{(\nu_i,\nu_j)\in K} \mathcal{C}(\mathcal{E}_{\nu_i - \nu_j})$ is the single-path capacity associated to the cut. Furthermore, for a network of distillable channels, Eq. (15) exactly coincides with Eq. (17), and we can write [13]

$$\mathcal{C}(\mathbf{N}) = \mathcal{C}(R^\star) = \min_C \mathcal{C}(C) = \min_C E_R(C). \tag{18}$$

Thanks to the extension of the definition of the entanglement cut to the lossy repeater scenario, we can still rely on the chain of equalities in Eq. (18). Using the quantum channel defined in Eq. (14), we can therefore define the capacity of the single route $R' \in \mathbf{R}'_{\mathbf{N}'}$ in the lossy-repeater network $\mathbf{N}'$ as

$$\mathcal{C}(R') := \min_{(\nu_i^2,\nu_j^2)\in R'} \mathcal{C}(\mathfrak{E}_{i,j}^{R'}). \tag{19}$$

We notice that the links (ν_0^1, ν_0^2) and (ν_N^2, ν_N^3) belong to any possible existing single-path route of the lossy-repeater network, but since in our model they are both associated to a noiseless quantum channel, they can be disregarded in the definition of the route capacity.

The main aim of our investigation is the analysis to the fundamental example of optical networks, where the link (ν_i^3, ν_j^1) connecting different nodes is described by a lossy channel with transmissivity $\eta_{i,j}$. We again assume that the two distinct quantum channels associated to the two internal repeater links (ν_i^1, ν_i^2) and (ν_i^2, ν_i^3) are represented by two lossy channels $\mathcal{E}_{\nu_i^1 - \nu_i^2}$ and $\mathcal{E}_{\nu_i^2 - \nu_i^3}$ with respective transmissivities r_i and t_i. As a consequence, the quantum channel $\mathfrak{E}_{i,j}$, describing the effect of the transmission over the generic node-fibre-node link (ν_i^2, ν_j^2), is a lossy channel with a transmissivity given by the product of the transmissivities of the involved lossy channels, i.e. $\mathcal{T}_{i,j} := \eta_{i,j} r_i t_j$ and capacity $\mathcal{C}(\mathfrak{E}_{i,j}) = -\log_2(1 - \mathcal{T}_{i,j})$.

It then follows that the generic route $R' \in \mathbf{R}'_{\mathbf{N}'}$ is identified by a collection of lossy channels with transmissivities $\{\mathcal{T}_{i,j}^{R'}\}$. By defining the transmissivity of route R' as

$$\widetilde{\mathcal{T}}^{R'} := \min_{(\nu_i^2,\nu_j^2)\in R'} \mathcal{T}_{i,j}^{R'}, \tag{20}$$

its capacity reads

$$\mathcal{C}(R') = -\log_2(1 - \widetilde{\mathcal{T}}^{R'}). \tag{21}$$

If we now maximize the expression in Eq. (21) over the route set $\mathbf{R}'_{\mathbf{N}'}$, we obtain the single-path capacity of the lossy-repeater quantum network

$$\mathcal{C}_{\text{loss}}(\mathbf{N}') := \max_{R'\in\mathbf{R}'_{\mathbf{N}'}} \mathcal{C}(R') = -\log_2(1 - \mathcal{T}), \tag{22}$$

$$\mathcal{T} := \max_{R'\in\mathbf{R}'_{\mathbf{N}'}} \widetilde{\mathcal{T}}^{R'}. \tag{23}$$

Equivalently, following the last terms of Eq. (18), we can compute the capacity by minimizing, over all the possible cuts C, either the capacity of an entanglement cut $\mathcal{C}(C)$ or the REE of an entanglement cut $E_R(C)$. Thus, we may consider

$$\begin{aligned} E_R(C) &:= \max_{(\nu_i^2,\nu_j^2)\in K} E_R(\rho_{\mathfrak{E}_{i,j}}) \\ &= \max_{(\nu_i^2,\nu_j^2)\in K} [-\log_2(1 - \mathcal{T}_{i,j})] \\ &= -\log_2(1 - \widetilde{\mathcal{T}}_C), \end{aligned} \tag{24}$$

with $\widetilde{\mathcal{T}}_C = \max_{(\nu_i^2,\nu_j^2)\in K} \mathcal{T}_{i,j}$. We then obtain the single-path capacity of the lossy-repeater network via the minimization

$$\mathcal{C}_{\text{loss}}(\mathbf{N}') = \min_C [-\log_2(1 - \widetilde{\mathcal{T}}_C)]. \tag{25}$$

By specifying Eqs. (22) and (25) to identical repeaters, i.e. $r_i = r_j = r$ and $t_i = t_j = t$, $\forall i, j = 0, \ldots, |V|$, we get

$$\mathcal{C}_{\text{loss}}(\mathbf{N}') = -\log_2[(1 - v \cdot \eta_{\mathbf{N}'})], \tag{26}$$

where we have defined $v := rt$ and

$$\eta_{\mathbf{N}'} := \max_{R'\in\mathbf{R}'_{\mathbf{N}'}} \min_{(\nu_i^2,\nu_j^2)} \eta_{i,j}^{R'} = \min_C \max_{(\nu_i^2,\nu_j^2)\in K} \eta_{i,j}. \tag{27}$$

The expressions above generalize the single-path capacity formulas of Ref. [13] from ideal to lossy repeaters.

E. Multi-path capacity of the lossy-repeater network

A powerful routing strategy in a network is represented by flooding, where systems are transmitted in parallel so that each edge is exploited in each network use. Let us consider a quantum network $\mathbf{N}'$ obtained, as described in the previous section, after node splitting $\mathbf{N} \to \mathbf{N}'$, with a corresponding graph $G' = (V', E')$ where $V' = \{(\nu_i^1, \nu_i^2, \nu_i^3)\}_{i=0,\cdots,N}$. Once an orientation to the network $\mathbf{N}'$ has been assigned, a multi-path flooding protocol can be defined as a collection of multicasts, each one realizing a point-to-multipoint communication. An orientation to the undirected network $\mathbf{N}$ is assigned by setting Alice $(\widehat{\nu_0})$ and Bob $(\widehat{\nu_N})$ respectively as the source and the sink of the network, and then by assigning a source-sink orientation to each edge of the network. Namely, for a generic link between the i-th and the j-th, we always identify ν_i^3 as the source and ν_j^1 as the sink. In this way a point-to-multipoint communication from node $\widehat{\nu_i}$ is defined as a quantum communication between $\widehat{\nu_i}$ and its out-neighborhood $D_{\widehat{\nu_i}}^{\text{out}} := \{\nu_j^1 \in V' | (\nu_i^3, \nu_j^1) \in E'_D\}$, with E'_D the edge-set E' where each element is now oriented. After the internal route $\widehat{\nu_0}$ at the sender's repeater station, the multi-path protocol starts with node ν_0^3 sending quantum systems to each repeater station belonging to its neighbourhood.

The converse upper bound for the multi-path capacity $\tilde{\mathcal{C}}(\mathbf{N})$ of a quantum network $\mathbf{N}$ is given by [13]

$$\tilde{\mathcal{C}}(\mathbf{N}) \leq \min_C \tilde{E}_R(C), \tag{28}$$

where the minimization is over all the possible cuts of the network and $\tilde{E}_R(C)$ is the multi-path REE flowing through an entanglement cut C. This is defined as the total REE of the cut set K associated to C, namely

$$\tilde{E}_R(C) := \sum_{(\nu_i,\nu_j)\in K} E_R(\rho_{\mathcal{E}_{i,j}}) \ . \tag{29}$$

An achievable rate (lower bound) for the multi-path capacity of the network is computed by applying the max-flow/min-cut theorem to the network, leading to [13]

$$\tilde{\mathcal{C}}(\mathbf{N}) \geq \min_C \tilde{\mathcal{C}}(C) \ , \tag{30}$$

where $\mathcal{C}(C)$ is the multi-path capacity of an entanglement cut, defined by

$$\tilde{\mathcal{C}}(C) := \sum_{(\nu_i,\nu_j)\in K} \mathcal{C}(\mathcal{E}_{\nu_i-\nu_j}) \ . \tag{31}$$

When the quantum network is connected by distillable quantum channels [10], the previous upper (28) and lower bound (30) coincide and the multi-path capacity satisfies the following chain of equalities

$$\tilde{\mathcal{C}}(\mathbf{N}) = \min_C \tilde{\mathcal{C}}(C) = \min_C \tilde{E}_R(C). \tag{32}$$

Again we are able to generalize the analytical formulas, by extending the multi-path capacity for quantum and private communication over a quantum network from ideal to imperfect lossy nodes. For the fundamental case of an optical network connected by lossy channels (e.g., fibres), the crucial decomposition is the one in Eq. (14), where all the channels involved are lossy channels and therefore distillable.

Combining our decomposition with Eq. (31), we compute the multi-path capacity of an entanglement cut by summing up over the capacities of the quantum channels $\mathfrak{E}_{i,j}$ associated with the cut set K. We then have

$$\begin{aligned}\tilde{\mathcal{C}}_{\text{loss}}(C) &= \sum_{(\widehat{\nu_i},\widehat{\nu_j})\in K} \mathcal{C}(\mathfrak{E}_{i,j}) \\ &= \sum_{(\widehat{\nu_i},\widehat{\nu_j})\in K} E_R(\rho_{\mathfrak{E}_{i,j}}) \\ &= \sum_{(\widehat{\nu_i},\widehat{\nu_j})\in K} -\log_2(1-\mathcal{T}_{i,j}) \\ &= -\log_2(L_C)\end{aligned} \tag{33}$$

where we have defined the total losses over a cut set as the product of the losses over the channels (repeater and link losses) in the cut set, i.e.

$$L_C := \prod_{(\widehat{\nu_i},\widehat{\nu_j})\in K} (1-\mathcal{T}_{i,j}). \tag{34}$$

Then the multi-path capacity of the quantum network with lossy repeaters is given by the minimization over all the possible entanglement cut of the above expression, i.e.,

$$\tilde{\mathcal{C}}_{\text{loss}}(\mathbf{N}') = \min_C \tilde{\mathcal{C}}_{\text{loss}}(C) \tag{35}$$

$$= -\log_2(\max_C L_C) \ . \tag{36}$$

It is easy to see that multi-path strategy is advantageous with respect to single-path even in the presence of lossy repeaters. For this purpose we can consider a split network $\mathbf{N}'$ with identical repeaters (i.e. same loss) at each node and where all the network links (ν_i^3, ν_j^1) are identical lossy channels with transmissivity η. Then from Eqs. (26) and (36), we get

$$\tilde{\mathcal{C}}_{\text{loss}}(\mathbf{N}') = -\log_2(1-\upsilon\eta)^m = m\mathcal{C}_{\text{loss}}(\mathbf{N}'), \tag{37}$$

where m is the number of network links of the smallest allowed cut set. For instance, in the diamond network $\mathbf{N}'_\diamond$ of Fig. 4 panel b), the value of m is equal to 2.

V. CONCLUSION AND OUTLOOK

Our work establishes analytical formulas for the maximum achievable rate of quantum and private communication between two end-users of a quantum network where the nodes are affected by internal loss. In the linear repeater chain scenario, we exploit a classical network technique, known as node splitting, to model the inevitable internal repeater loss. In this way, we are able to describe the repeater chain as a suitable collection of distillable quantum channels, i.e. channels for which the lower and the upper bounds on the two-way assisted quantum (and private) capacity coincide.

Given this setting, by employing the powerful methodology of channel simulation and teleportation stretching, we have established an exact expression for the lossy-repeater capacity for quantum communication over a network with arbitrary number of lossy repeaters connected by pure-loss channels. Interestingly, when the number of repeaters increases, the derived capacity turns out to be a function of the internal loss of a single node, which then acts as the ultimate upper limit to the maximum achievable rate for quantum and private communication.

Finally, we have considered the important role played by *time* that must be taken into account in any actual implementation of a quantum repeater chain. In such a realistic setting, we have shown how the performance can indeed overcome the repeaterless PLOB bound and approach the optimal single-repeater bound, even in the presence of internal time-dependent loss, e.g., induced by limited coherence times.

The present study can be seen as a relevant step in an important direction and invites further studies in many ways. This work has put an emphasis on losses, which in most practical implementations is indeed the main source of errors. A more detailed study should accommodate dark counts and further offset noise as well. On a broader level, the work hopes to push forward a line of thought aiming at identifying the ultimate bounds for practically achievable rates in quantum repeater schemes, without going too much into specifics of a particular implementation. Such considerations, so is reasonably to expect, substantially help assessing the potential of multi-partite long-distance quantum communication.

VI. ACKNOWLEDGMENTS

J. E. has been supported by the BMBF (QR.X on quantum repeaters) and the Einstein Foundation. R. L. acknowledges support from the Alexander von Humboldt Foundation. N. W. has been funded by a Marie Sklodowska-Curie Individual Fellowship. S. P. has been supported by the European Union via "Continuous Variable Quantum Communications" (CiViQ, Grant Agreement No. 820466). The authors would like to thank Frederik Hahn, Julius Wallnöfer and Peter van Loock for interesting discussions.

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, et al., Adv. Opt. Photon. **12**, 1012 (2020).
[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, Nature Phot. **9**, 641 (2015).
[5] C. Portmann and R. Renner, arXiv:2102.00021 (2021).
[6] S. Khatri and M. M. Wilde, arXiv:2011.04672 (2021).
[7] R. F. Werner, *Quantum information theory — an invitation* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2001), pp. 14–57.
[8] J. S. Sidhu, S. K. Joshi, M. Gündoğan, T. Brougham, D. Lowndes, L. Mazzarella, M. Krutzik, S. Mohapatra, D. Dequal, G. Vallone, et al., IET Quantum Communication **93**, 1– 36 (2021).
[9] M. Razavi, *An Introduction to Quantum Communications Networks*, 2053-2571 (Morgan & Claypool Publishers, 2018).
[10] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nature Comm. **8**, 15043 (2017).
[11] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).
[12] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[13] S. Pirandola, Commun. Phys. **2**, 51 (2019), see also arXiv:1601.00966.
[14] H. J. Kimble, Nature **453**, 1023 (2008).
[15] T. Satoh, K. Ishizaki, S. Nagayama, and R. Van Meter, Phys. Rev. A **93**, 032302 (2016).
[16] M. Epping, H. Kampermann, and Bruß, New J. Phys. **18**, 053036 (2016).
[17] F. Hahn, A. Pappa, and J. Eisert, npj Quantum Inf. **5**, 76 (2019).
[18] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpedek, M. Skrzypczyk, et al., Commun. Phys. **4**, 164 (2021).
[19] K. Goodenough, D. Elkouss, and S. Wehner, Phys. Rev. A **103**, 032610 (2021).
[20] J. Eisert and M. M. Wolf, *Gaussian quantum channels* (Imperial College Press, London, 2007), pp. 23–42, arXiv:quant-ph/0505151.
[21] M. Hosseini, B. M. Sparkes, G. Campbell, P. K. Lam, and B. C. Buchler, Nature Comm. **2**, 174 (2011).
[22] N. Bernardes, L. Praxmeyer, and P. van Loock, Phys. Rev. A **83**, 012323 (2011).
[23] E. Shchukin, F. Schmidt, and P. van Loock, Phys. Rev. A **100**, 032322 (2019).
[24] P. van Loock, W. Alt, C. Becher, O. Benson, H. Boche, C. Deppe, J. Eschner, S. Höfling, D. Meschede, P. Michler, et al., Adv. Quant. Tech. **3**, 1900141 (2020).
[25] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, et al., Nature **580**, 60 (2020).
[26] Y. Pu, S. Zhang, Y. Wu, N. Jiang, W. Chang, C. Li, and L. Duan, arXiv.org (2021), 2101.08541.
[27] E. Campbell and J. Eisert, **108**, 020501 (2012).
[28] J. Dias and T. C. Ralph, Phys. Rev. A **95**, 022312 (2017).
[29] F. Furrer and W. J. Munro, Phys. Rev. A **98**, 032335 (2018).
[30] J. Dias, W. J. Munro, T. C. Ralph, and K. Nemoto (2019), arXiv:1906.06019.
[31] T. C. Ralph and A. P. Lund, *Quantum Communication Measurement and Computing Proceedings of 9th International Conference* p. 155 (2009).
[32] G. Xiang, T. Ralph, A. Lund, N. Walk, and G. Pryde, Nature Phot. **4**, 316 (2010).
[33] S. Pandey, Z. Jiang, J. Combes, and C. M. Caves, Phys. Rev. A **88**, 033852 (2013).
[34] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).
[35] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).
[36] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, Phys. Rev. Lett. **102**, 210501 (2009).
[37] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).
[38] I. Devetak, M. Junge, C. King, and M. B. Ruskai, Commun. Math. Phys **266**, 37 (2006).
[39] M. Hayashi, Springer-Verlag (2017).
[40] I. Devetak and A. Winter, Proc. Roy. Soc. A **461** (2003).
[41] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[42] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
[43] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[44] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

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

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

Appendix

Appendix A: Two-way quantum capacities and general bounds

The most important point-to-point quantum communication scenario concerns two remote parties, Alice and Bob, which are connected by a (memoryless) quantum channel $\mathcal{E}$ without pre-sharing any entanglement. By means of this channel, the two parties may implement various quantum tasks as for instance the reliable transmission of qubits, the distillation of entanglement bits (ebits) and the generation of secret bits. The most general protocols are based on transmissions through the quantum channel which are interleaved by local operations (LO) assisted by unlimited and two-way classical communication (CC), briefly called adaptive LOCCs. At the beginning of this protocol, Alice and Bob have two local registers a and b of quantum systems which are adaptively updated before and after each transmission through $\mathcal{E}$. After a number n of channel's uses, Alice and Bob will share the quantum state $\rho^n_{a,b}$ which depends on the sequence of LOCCs $\mathcal{L} = \{L_1, L_2, \cdots, L_n\}$.

The rate R_n of this protocol is defined through a target state ϕ_n whose content of information is equal to nR_n bits. If the output state $\rho^n_{a,b}$ is close in the trace norm to ϕ_n, i.e. $\|\rho^n_{a,b} - \phi_n\| \leq \epsilon$ for some $\epsilon \rightarrow> 0$, then the rate of the protocol is equal to R_n. The generic two-way capacity $\mathcal{C}(\mathcal{E})$ is defined by taking the limit for a large number of channel's uses n and by optimizing over all the possible adaptive protocols $\mathcal{L}$, i.e.

$$\mathcal{C}(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n \to \infty} R_n \; . \tag{38}$$

In order for the quantity $\mathcal{C}(\mathcal{E})$ to get an operational meaning, we need to specify the goal of the adaptive protocol implemented by Alice and Bob. Thus, if the target state is a maximally entangled state, meaning that the protocol is an entanglement distribution protocol, we have that $\mathcal{C}(\mathcal{E}) = D_2(\mathcal{E})$, where $D_2(\mathcal{E})$ is the two-way entanglement distribution capacity of the channel. Since an ebit can teleport a qubit and viceversa with a qubit is possible distribute an ebit, $D_2(\mathcal{E})$ is equal to the two-way quantum capacity $Q_2(\mathcal{E})$, i.e. the maximum achievable rate for transmitting quantum information. If the protocol is a QKD protocol, ϕ_n is a private state and the generic two-way quantum capacity is the secret key capacity $K(\mathcal{E})$ which is equal to the private capacity $P_2(\mathcal{E})$ (unlimited two-way CCs and one time-pad). Since a maximally entangled state is a specific type of private state, we can write the following relations between all the different capacities

$$Q_2(\mathcal{E}) = D_2(\mathcal{E}) \leq P_2(\mathcal{E}) = K(\mathcal{E}) \; . \tag{39}$$

As one can see from Eq. (38), the quantity $\mathcal{C}(\mathcal{E})$ cannot be evaluated directly from its definition and the best strategy to assess it is to resort to suitable lower and upper bounds that are usually built upon information and entanglement measures.

A general lower bound can be given in terms of the *coherent* [34, 35] or *reverse coherent information* [36, 37] which are, respectively, defined as

$$I_C(\mathcal{E}, \rho_A) = I(A\langle B)_{\rho_{RB}} := S(\rho_B) - S(\rho_{RB}), \tag{40}$$

$$I_{RC}(\mathcal{E}, \rho_A) = I(A\rangle B)_{\rho_{RB}} := S(\rho_R) - S(\rho_{RB}), \tag{41}$$

where the quantum channel $\mathcal{E}$ takes as an input the quantum state ρ_A of system A (see also the related notions of *negative cb-entropy* of a channel [38] and *pseudo-coherent information* [39]). If R is an auxiliary system and $|\psi\rangle_{RA}$ the purification of ρ_A, then the output of the channel is $\rho_{RB} = (\mathcal{I} \otimes \mathcal{E})(|\psi\rangle\langle\psi|_{RA})$. In the above expressions, we also have $\rho_{R(B)} = \mathrm{Tr}_{B(R)}\, \rho_{RB}$ and $S(\rho) := -\mathrm{Tr}(\rho \log_2 \rho)$ is the *von Neumann entropy*. When the input state ρ_A is a maximally-mixed state, its purification is a maximally-entangled state Φ_{RA}, so that ρ_{RB} becomes the Choi matrix of the channel $\sigma_{\mathcal{E}} = (\mathcal{I} \otimes \mathcal{E})(\Phi_{RA})$. Then we can define the coherent and reverse coherent information of the quantum channel $\mathcal{E}$ respectively as follows [10, Supp. Note 2]

$$I_C(\mathcal{E}) := I(A\langle B)_{\sigma_{\mathcal{E}}}, \tag{42}$$

$$I_{RC}(\mathcal{E}) := I(A\rangle B)_{\sigma_{\mathcal{E}}}. \tag{43}$$

The quantity $I_C(\mathcal{E})$ constitutes an achievable rate for *forward* one-way entanglement distillation, whereas $I_{RC}(\mathcal{E})$ is an achievable rate for *backward* one-way entanglement distillation. In fact, due to the *hashing inequality* [40], we can write

$$\max\{I_C(\mathcal{E}), I_{RC}(\mathcal{E})\} \leq D_1(\sigma_{\mathcal{E}}) \; , \tag{44}$$

where $D_1(\sigma_{\mathcal{E}})$ is the entanglement that can be distilled from the channel's Choi matrix with the assistance of forward or backward classical communication.

The general weak converse upper bound to the two-way quantum capacity $\mathcal{C}(\mathcal{E})$ derived in Ref. [10], is built upon the notion of the *relative entropy of entanglement* (REE) [41] suitably extended from quantum states to quantum channels. Let us recall that the REE of a quantum state ρ is defined as the minimum relative entropy between ρ and a separable state σ_s [41, 42], i.e.,

$$E_R(\rho) := \inf_{\sigma_s \in \mathrm{SEP}} S(\rho \| \sigma_s) \; . \tag{45}$$

We can also introduce the REE of a discrete variable quantum channel $\mathcal{E}$ with associated Choi matrix $\sigma_{\mathcal{E}}$ in the following way

$$E_R(\mathcal{E}) := \sup_{\rho} E_R[(\mathcal{I} \otimes \mathcal{E})(\rho)] \leq E_R(\sigma_{\mathcal{E}}) \; . \tag{46}$$

Then Ref. [10, Th. 1] states that generic two-way capacity of equation (38) is upper bounded by the REE bound

$$\mathcal{C}(\mathcal{E}) \leq E^{\star}_R(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n \to \infty} \frac{E_R(\rho^n_{a,b})}{n} \; , \tag{47}$$

where $\rho^n_{a,b}$ is the output state of a n-use adaptive protocol $\mathcal{L}$. Note that both the lower bound (44) and the upper bound (47) hold for an arbitrary quantum channel in arbitrary dimension. In the subsequent section, we discuss how to extend them to asymptotic states, providing in this way a formulation for CV systems, following the asymptotic methodology of Ref. [10].

Appendix B: Asymptotic formulation for bosonic systems

It is important to note that when dealing with continuous variable systems the maximally entangled state is an asymptotic state (energy-unbounded) obtained as the limit $\Phi := \lim_\mu \Phi^\mu$, where Φ^μ is a sequence of two mode squeezed vacuum (TMSV) states parametrized by μ which quantifies both the two-mode squeezing and the mean number $\bar{n}$ of thermal photons (local energy) in both modes, i.e., $\mu = \bar{n} + 1/2$ [43, 44]. According to this, the Choi state of a bosonic channel $\mathcal{E}$ (e.g. the pure-loss channel under consideration) is given by the asymptotic limit

$$\sigma_{\mathcal{E}} := \lim_\mu \sigma^\mu_{\mathcal{E}}, \quad \sigma^\mu_{\mathcal{E}} := (\mathcal{I} \otimes \mathcal{E})(\Phi^\mu) \ . \tag{48}$$

Correspondingly the computation of the (reverse) coherent information of a quantum channel introduced in Eq. (42) and (43) has to be performed as the following limits

$$I(A\langle B)_{\sigma_{\mathcal{E}}} := \lim_{\mu\to\infty} I(A\langle B)_{\sigma^\mu_{\mathcal{E}}}, \tag{49}$$

$$I(A\rangle B)_{\sigma_{\mathcal{E}}} := \lim_{\mu\to\infty} I(A\rangle B)_{\sigma^\mu_{\mathcal{E}}} \ . \tag{50}$$

For *bosonic Gaussian channels* [20], it can be shown that the functionals $I(A\langle B)_{\sigma^\mu_{\mathcal{E}}}$ and $I(A\rangle B)_{\sigma^\mu_{\mathcal{E}}}$ are continuous, monotonic and bounded in μ. Therefore, the above limits are finite and we can continuously extend Eq. (44) to the asymptotic Choi matrix of a CV channel, for which we may set $D_1(\mathcal{E}) := \lim_{\mu\to\infty} D_1(\sigma^\mu_{\mathcal{E}})$.
Let us now consider two sequences of states ρ^μ_1 and ρ^μ_2 converging, respectively, in the trace norm to ρ_1 and ρ_2, i.e., $\|\rho^\mu_i - \rho_i\| \to 0$, for $i = 1, 2$. By exploiting the lower semicontinuity of the relative entropy, we can write

$$S(\rho_1\|\rho_2) \leq \liminf_{\mu\to\infty} S(\rho^\mu_1\|\rho^\mu_2) \ . \tag{51}$$

As a consequence the relative entropy of entanglement of an asymptotic state $\rho = \lim_\mu \rho^\mu$ is defined as follows

$$E_R(\rho) := \inf_{\rho^\mu_s} \liminf_{\mu\to\infty} S(\rho^\mu\|\rho^\mu_s) \ , \tag{52}$$

where ρ^μ_s is an arbitrary sequence of separable states satisfying $\|\rho^\mu_s - \rho_s\| \overset{\mu\to\infty}{\longrightarrow} 0$ for some separable state ρ_s. A direct implication of Eq. (52) is that the REE computed over the *quasi*-Choi matrix $\sigma^\mu_{\mathcal{E}}$ of a bosonic channel is defined as

$$E_R(\sigma_{\mathcal{E}}) := \inf_{\rho^\mu_s} \liminf_{\mu\to+\infty} S(\sigma^\mu_{\mathcal{E}}\|\rho^\mu_s) \tag{53}$$

Appendix C: Channel simulation and teleportation stretching

We already mentioned that in order to write Eq. (4), which is fundamental in simplifying the REE bound of Eq. (47), we need to rely on two ingredients which are, respectively, known as *channel simulation* and *teleportation stretching*. In this section we briefly review these two technical steps with the main definitions while referring the reader to [10] for more technical details and a discussion of historical developments.

The notion of quantum channel simulation comes from a straightforward generalization of quantum teleportation protocol whose structure involves local operations (LO), Bell detection on Alice's side and Bob's unitary correction, plus classical communication (CC) from Alice to Bob [45]. For a maximally entangled resource state Φ, the teleported output perfectly correspond to the input. If we perform teleportation over an arbitrary mixed resource state of systems A and B, the teleported state on Bob's side will result in the output of a certain quantum channel $\mathcal{E}$ from Alice to Bob (see Ref. [46, Sec. V] for the initial insights of this technique, later expanded by various groups over the years).

More generally, any implementation through an arbitrary LOCC $\mathbb{L}$ and a resource state σ simulates the output of a quantum channel $\mathcal{E}$. Thus, for any $\mathcal{E}$ and for any input ρ, we can express the output as [10]

$$\mathcal{E}(\rho) = \mathbb{L}(\rho \otimes \sigma) \ . \tag{54}$$

When dealing with CV systems as in our scenario, the LOCC simulation involves the limit $\sigma := \lim_{\mu\to\infty} \sigma^\mu$ of resource states σ^μ. Then, for any finite μ, the simulation provides the approximated channel

$$\mathcal{E}^\mu(\rho) = \mathbb{L}(\rho \otimes \sigma^\mu) \ , \tag{55}$$

which defines the quantum channel $\mathcal{E}$ as the following pointwise limit

$$\mathcal{E}(\rho) = \lim_{\mu\to\infty} \mathcal{E}^\mu(\rho) \ . \tag{56}$$

For any given quantum channel, we can always find a suitable LOCC $\mathbb{L}$ and a resource state σ that achieve the simulation in Eq. (54). A genuine LOCC simulation is established when the quantum channel satisfies the property of *teleportation covariance*. If $\mathcal{U}$ is the group of teleportation unitaries, a quantum channel $\mathcal{E}$ is teleportation covariant if the following identity holds for any $U \in \mathcal{U}$

$$\mathcal{E}(U\rho U^\dagger) = V\mathcal{E}(\rho)V^\dagger \ , \tag{57}$$

with V a unitary transformation not necessarily belonging to $\mathcal{U}$. Note that the unitary group $\mathcal{U}$ is the Weyl-Heisenberg group (generalized Pauli operators) for DV systems, while for CV systems it coincides with the group of displacement operators. An interesting property of a tele-covariant quantum channel $\mathcal{E}$ is that it can be simulated by teleporting the input state ρ using its Choi matrix $\sigma_{\mathcal{E}}$ as the resource for teleportation, i.e., for a DV channel we write

$$\mathcal{E}(\rho) = \mathbb{T}(\rho \otimes \sigma_{\mathcal{E}}) \tag{58}$$

where $\mathbb{T}$ is teleportation [45]. For a CV channel, by recalling Eq. (56), the above relation is rewritten as

$$\mathcal{E}^{\mu}(\rho) = \mathbb{T}(\rho \otimes \sigma^{\mu}_{\mathcal{E}}) \ , \tag{59}$$

where now $\mathbb{T}$ is the Braunstein-Kimble teleportation [4, 43] and the asymptotic Choi state $\sigma^{\mu}_{\mathcal{E}}$ defines the asymptotic Choi state for large μ as in Eq. (48). Note that several quantum channels satisfy the property of teleportation covariance, including Pauli and erasure channels in DVs, and bosonic Gaussian channels in CVs.

By making use of channel simulation, we are able to perform teleportation stretching and to simplify the adaptive structure of a protocol for quantum and private communication. This means that the protocol output $\rho^{n}_{a,b}$ is reduced into an n-fold tensor product of resource states $\sigma^{\otimes n}$ up to a TP LOCC $\bar{\Lambda}$. The reduction procedure starts by replacing each transmission over the channel $\mathcal{E}$ with its simulation $(\mathbb{T}, \sigma)$. At this stage, we can then stretch the resource state σ outside the adaptive operations, while $\mathbb{T}$ is incorporated into the protocol LOCCs. After that, all the LOCCs together with the initial register preparation, are merged into a single final LOCC $\bar{\Lambda}$, which turns out to be TP after averaging over all the possible local measurement outcomes. At the end we can then write [10, Lemma 3]

$$\rho^{n}_{a,b} = \bar{\Lambda}(\sigma^{\otimes n}) \ . \tag{60}$$

For CV quantum channels, the above equation must be interpreted in an asymptotic fashion in the following manner. We replace each transmission through $\mathcal{E}$ with the channel $\mathcal{E}^{\mu}$ defined in (59) with a finite-energy resource state σ^{μ}. If we assume that the local registers of Alice and Bob have energy $\leq N$, i.e., the total input state of each transmission belongs to a bounded alphabet D_N, the channel $\mathcal{E}^{\mu}$ simulates $\mathcal{E}$ up to an error given by $\epsilon(\mu, N) := \|\mathcal{E} - \mathcal{E}^{\mu}\|_{\diamond N}$, where

$$\|\mathcal{E} - \mathcal{E}'\|_{\diamond N} := \sum_{\rho_{RS} \in D_N} \|\mathcal{I}_R \otimes \mathcal{E}_S(\rho_{RS}) - \mathcal{I}_R \otimes \mathcal{E}'_S(\rho_{RS})\| \tag{61}$$

is the energy constrained diamond norm. By exploiting the non-increasing of the trace distance under CPTP maps and the triangle inequality, it can be proven [10] that the trace distance between the output $\rho^{n}_{a,b}$ and the simulated output $\rho^{n,\mu}_{a,b}$ (the output of an adaptive protocol performed over $\mathcal{E}^{\mu}$) satisfies

$$\|\rho^{n}_{a,b} - \rho^{n,\mu}_{a,b}\| \leq n\epsilon(\mu, N) \ . \tag{62}$$

We can now substitute $\rho^{n,\mu}_{a,b}$ with its decomposition given by the teleportation stretching, so that we obtain

$$\|\rho^{n}_{a,b} - \bar{\Lambda}(\sigma^{\mu \otimes n})\| \leq n\epsilon(\mu, N) \ , \tag{63}$$

for any energy constrain N. Then by taking the limit for $\mu \to \infty$ we get the asymptotic version of Eq. (4) (asymptotic stretching)

$$\lim_{\mu \to \infty} \|\rho^{n}_{a,b} - \bar{\Lambda}(\sigma^{\mu \otimes n})\| = 0 \ . \tag{64}$$

By using the decompositions of Eq. (60) and (64) we can consequently simplify the upper bound in (15). In fact we can write

$$E_R(\rho^{n}_{a,b}) \leq E_R(\sigma^{\otimes n}) \leq nE_R(\sigma) \ , \tag{65}$$

where in the two inequalities the monotonicity of the REE under TP LOCCs and the sub-additivity of the REE over tensor products are, respectively, exploited. By putting Eq. (65) into Eq. (15), we can get rid of both the optimization over all the adaptive protocols and the asymptotic limit so that a *single-letter* upper bound to the capacities introduced in (39) is obtained

$$\mathcal{C}(\mathcal{E}) \leq E_R(\sigma) \ . \tag{66}$$

If the channel is teleportation covariant we can then write the above equation in terms of the Choi matrix $\sigma_{\mathcal{E}}$ of the channel, i.e.,

$$\mathcal{C}(\mathcal{E}) \leq E_R(\sigma_{\mathcal{E}}) \ . \tag{67}$$

See also Ref. [10, Th. 5] and related proofs for more details.

Appendix D: BB84 key rate

Over a pure loss channel there is no dephasing so there is one bit of distillable key for every successful connection between the two remote stations. All that is required then is to calculate the probability of this happening for a single channel use for a repeater scheme based upon storage and entanglement swapping, but without any distillation. Following Ref. [24] we can calculate that, for a scheme with a half-link success probability, p, given by (12) and symmetric transmission and receiver losses $\tau^{t,\mathrm{eff}} = \tau^{r,\mathrm{eff}} = \tau^{\mathrm{eff}}$ that the BB84 rate is

$$r_{\mathrm{BB84}} = \frac{1}{2}\frac{\sqrt{\eta}\tau^{\mathrm{eff}}(2 - \sqrt{\eta}\tau^{\mathrm{eff}})}{3 - 2\sqrt{\eta}\tau^{\mathrm{eff}}}\tau_{\mathrm{mem}}. \tag{68}$$

The rate per time is then given by Rr_{BB84}. For a standard polarisation based implementation, there are actually two optical modes available (corresponding to horizontal and vertical polarisation) that must be transmitted for each round, so this rate must be halved to get the rate per transmitted mode, which gives the factor of $1/2$ in the above expression.