ARTICLE OPEN

Check for updates

Achieving the ultimate end-to-end rates of lossy quantum communication networks

Matthew S. Winnel[1]✉, Joshua J. Guanzon[1], Nedasadat Hosseinidehaj[1] and Timothy C. Ralph[1]

The field of quantum communications promises the faithful distribution of quantum information, quantum entanglement, and absolutely secret keys, however, the highest rates of these tasks are fundamentally limited by the transmission distance between quantum repeaters. The ultimate end-to-end rates of quantum communication networks are known to be achievable by an optimal entanglement distillation protocol followed by teleportation. In this work, we give a practical design for this achievability. Our ultimate design is an iterative approach, where each purification step operates on shared entangled states and detects loss errors at the highest rates allowed by physics. As a simpler design, we show that the first round of iterations can purify completely at high rates. We propose an experimental implementation using linear optics and photon-number measurements which is robust to inefficient operations and measurements, showcasing its near-term potential for real-world practical applications.

npj Quantum Information (2022)8:129 ; https://doi.org/10.1038/s41534-022-00641-0

INTRODUCTION

The great challenge for quantum communication[1] is how to overcome loss[2], the dominant source of noise through free space and telecom fibres. Many applications[3–7], including quantum key distribution (QKD)[8,9] (i.e., the task of sharing a secret random key between two distant parties), suffer from an exponential rate-distance scaling[10,11]. Determining the most efficient protocols for distributing quantum information, entanglement, and secure keys is of vital importance to realise the full capability of the quantum internet[12].

It is known that the reverse coherent information (RCI)[13] is an achievable rate for entanglement distillation by an implicit optimal protocol based on one-way classical communication. For the bosonic pure-loss channel, this rate is $R = -\log_2(1-\eta)$[10], where $\eta \in [0, 1]$ is the channel transmissivity. This is an achievable rate for entanglement distillation, E_D, over the lossy channel and is also an achievable rate for secret key distribution, K, since an ebit is a specific form of secret key bit. To summarise, we have $K \geq E_D \geq R = -\log_2(1-\eta)$. Ref. [14] proved the upper bound, the so-called Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound, that is, $K \leq -\log_2(1-\eta)$. This, together with the lower bound, R, from ref. [10], establishes $K = E_D = R = -\log_2(1-\eta) = C$, the two-way-assisted entanglement distribution capacity and secret key distribution capacity of the pure-loss channel.

Likewise, there are fundamental limits to the highest end-to-end rates of arbitrary quantum communication networks[15], where untrusted quantum repeaters divide the total distances into shorter quantum channels (links). Quantum repeaters are strictly required to beat the PLOB bound[16,17]. For a linear repeater chain, it is optimal to place repeaters equidistantly, then the ultimate end-to-end rate is given by $-\log_2(1-\eta)$[15], where η now refers to the transmissivity of each link. For a multiband network, consisting of m generally entangled channels in parallel, the rate is additive, $-m\log_2(1-\eta)$[15]. These ultimate repeater bounds are achievable by using an optimal entanglement distillation protocol followed by quantum teleportation (entanglement swapping), while ideal quantum memories are most likely required to achieve the highest rates.

The goal of this paper is to give a physical realisation for achieving these ultimate rates, which could pave the way for experimental implementations. While the highest achievable secret key rate for point-to-point CV QKD saturates the PLOB bound[8], it does not provide a physical design for entanglement distillation. Furthermore, it is impossible to distil Gaussian entanglement using Gaussian operations only[18,19] so quantum repeaters must use non-Gaussian elements[20].

Protocols based on infinite-dimensional systems are required to saturate the ultimate limits. However, the majority of quantum-information-processing tasks and techniques are for discrete-variable (DV) systems[21] where the quantum information is finite-dimensional. In contrast, for continuous-variable (CV) systems[2,22–24], the quantum information is infinite-dimensional and encoded in the quadrature amplitudes, and in principle offer easier state manipulation[22] and compatibility with existing optical telecom infrastructure[25]. Previous practical quantum repeater designs are unable to distil entanglement at the ultimate rates[26–31].

Quantum repeaters have previously been categorised into three generations depending on how they combat loss and other sources of noise[16,17]. With respect to CV systems, the first two generations remove loss via teleportation-based techniques, for instance, entanglement swapping and/or noiseless linear amplification[32–38]. These techniques fail to achieve the ultimate limits under pure loss since the output state is not pure and the success probability is zero for high-energy input states. For instance, the schemes based on noiseless linear amplification[29–31] have the same rate-distance scaling as the ultimate bounds but do not saturate them. A simple explanation is given in Supplementary Note 1, also see ref. [39].

The third generation of quantum repeaters[40] uses quantum error correction and is a purely one-way communication scheme. It promises high rates since it does not require back-and-forth

[1]Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, St Lucia, QLD 4072, Australia.
✉email: mattwinnel@gmail.com

classical signalling, however, here the ultimate rates are bounded by the unassisted quantum capacity of each link[14], $\log_2(\frac{\eta}{1-\eta}) < C$. This means the third-generation rate is zero if $\eta \leq 0.5$, which translates to a maximum link distance of about 15 km for optical fibre with a loss rate of 0.2 dB km^{-1}. In contrast, the two-way assisted capacity of pure loss allows a nonzero achievable rate at all distances. It is interesting to note that the family of GKP codes[41] achieves the unassisted capacity of general Gaussian thermal-loss channels with added thermal noise, where pure loss is the zero-temperature case, up to at most a constant gap[42]. Likewise, our main result is to give a practical protocol that achieves the two-way assisted capacity of the pure-loss channel.

In summary, all three generations of quantum repeaters are unable to operate at rates that saturate the ultimate limits of quantum communications. Motivated by this reality, we introduce an iterative protocol to purify completely from pure loss and achieve the capacity of the channel. Our schemes are inspired by refs. [43,44]. The idea is that neighbouring nodes locally perform photon-number measurements on copies of shared CV entanglement across the lossy channel, followed by two-way classical communication to compare photon-number outcomes. We show that the highest rates of our purification scheme, requiring two-way classical communication, achieve the fundamental limits of quantum communications for pure-loss channels. In contrast to quantum error correction, we describe purification as a quantum-error-detection scheme against loss. We consider a much-simpler design with good rates requiring only one-way classical communication and no iteration.

In this work, the required measurements are quantum non-demolition measurements (QND) of the total photon number of multiple modes and can be implemented experimentally using linear optics and photon-number measurements. This implementation is naturally robust against the inefficiencies of the detectors and gates. Alternatively, these QND measurements can be implemented using high finesse cavities and cross-Kerr nonlinearities[44].

RESULTS

First, we introduce our iterative protocol for the complete purification of high-dimensional entanglement, saturating the two-way assisted capacity of the bosonic pure-loss channel. Then, we show that our protocol without iteration (i.e. single-shot) still gives high rates which fall short of the ultimate limits by at worst a factor of 0.24. Finally, we explain how to implement our protocol using linear optics and photon-number measurements.

Iterative purification

Alice and Bob share multiple copies of a state which is entangled in photon number, such that in a lossless situation they will always measure the same number of photons. Our purification technique, in a pure loss situation, is for Alice and Bob to each locally count the total number of photons contained in multiple copies of the shared entangled states, and then compare the results. If they locally find a different total number of photons, this means photons were lost. Alice and Bob then iteratively perform total photon-number measurements over smaller subsets of states until their outcomes are the same, and hence distil pure entanglement. We prove that the highest average rate of the protocol achieves the capacity of the pure-loss channel.

We now consider our protocol in detail. The protocol is shown in Fig. 1. Consider two neighbouring nodes in a network, Alice and Bob, separated by a repeaterless link. Round one of our iterative protocol is identical to the entanglement purification of Gaussian CV quantum states from ref. [44], however, our protocol includes an iterative procedure. Alice prepares m copies of a pure two-mode squeezed vacuum (TMSV) state, $|\chi\rangle = \sqrt{1-\chi^2}\sum_{n=0}^{\infty}\chi^n|n\rangle|n\rangle$ in the Fock photon-number basis, with squeezing parameter

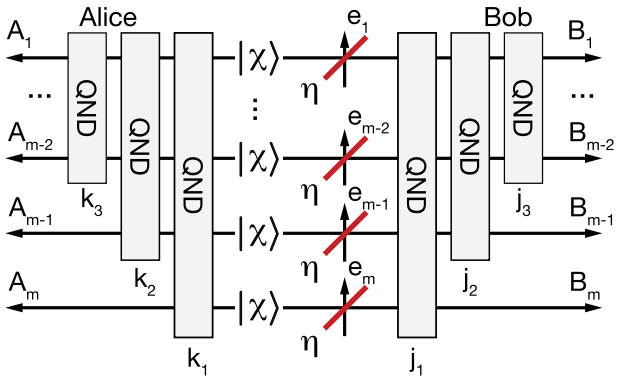

Fig. 1 Our iterative protocol for the complete purification of Gaussian continuous-variable quantum states. Alice shares m two-mode-squeezed-vacuum states with Bob across independent pure-loss channels with transmissivity η. Iterative QND measurements of total photon number at Alice's and Bob's sides followed by classical communication herald pure states whenever $k_n = j_n$, which means round n is successful and the protocol is complete. The highest average rate of quantum communication achieves the capacity (the PLOB bound[14]). Alice's measurements encode the quantum information onto the rails, and Bob's measurements purify the entanglement and decode the quantum information.

$\chi \in [0, 1]$. The unique entanglement measure, E, for a bipartite pure state, $|\phi\rangle$, is given by the von Neumann entropy, S, of the reduced state, i.e., $E = -\mathrm{tr}(\rho_A \log_2 \rho_A)$, where $\rho_A = \mathrm{tr}_B|\phi\rangle\langle\phi|$. This means Alice initially prepares mE_χ ebits of entanglement, where $E_\chi = G[(\lambda_k - 1)/2]$, where $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$, $\lambda_k = 2\bar{n} + 1$, $\bar{n} = \sinh^2 r$, and $r = \tanh^{-1}\chi$.

Alice shares the second mode of each of the m pairs with Bob across the link. The error channel we consider is bosonic pure loss, modelled by mixing the data rails with vacuum modes of the environment, or a potential eavesdropper (Eve), on a beamsplitter with transmissivity η.

Alice encodes the quantum information into a quantum-error-detecting code so that Bob can detect errors on his side. To do this, she performs a QND measurement of total photon number on the m modes and obtains outcome k_1 (where subscript 1 refers to round one of iteration), and shares this information with Bob via classical communication. Alice's measurement projects the system before the channel onto a maximally-entangled state[44]

$$|\phi_{k_1,m}\rangle_{AB} = (1-\chi^2)^{\frac{m}{2}}\chi^{k_1}\sum_{n_1,n_2,\cdots,n_m}^{n_1+n_2+\cdots+n_m=k_1}|n_1,n_2,\cdots,n_m\rangle_A|n_1,n_2,\cdots,n_m\rangle_B \quad (1)$$

$$= (1-\chi^2)^{\frac{m}{2}}\chi^{k_1}\sum_{\mu=0}^{d_{k_1,m}-1}|\mu_{k_1,m}\rangle_A|\mu_{k_1,m}\rangle_B, \quad (2)$$

where $|\mu_{k_1,m}\rangle = |n_1^{(\mu)}, n_2^{(\mu)}, \cdots, n_m^{(\mu)}\rangle$ can be viewed as orthogonal basis states which form a quantum-error-detecting code, each composed of $\sum_{i=1}^{m} n_i^{(\mu)} = k_1$ photons. We discuss the code in detail later. The pure maximally entangled state $|\phi_{k_1,m}\rangle_{AB}$ has entanglement $E_{k_1,m} = \log_2 d_{k_1,m}$ ebits with dimension $d_{k_1,m} = \binom{k_1+m-1}{k_1}$, and the probability of Alice's measurement outcome, k_1, is $P^{\mathrm{Alice}}_{k_1,m} = (1-\chi^2)^m\chi^{2k_1}d_{k_1,m}$. The dimension, $d_{k_1,m}$, is the total number of ways k_1 identical photons can be arranged among the m distinct rails.

Bob then performs a QND measurement of the total photon number across the m rails on his side to detect loss errors. If Bob obtains the outcome j_1 photons and knows that Alice sent k_1 photons, then both Alice and Bob know that $k_1 - j_1$ photons were lost. Bob's QND measurement, with success probability

$P^{\mathrm{Bob}}_{k_1,j_1} = (1-\eta)^{k_1-j_1}\eta^{j_1}\binom{k_1}{j_1}$, heralds a renormalised mixed state shared between Alice and Bob which does not depend on loss for any outcome j_1. That is, together Alice's and Bob's QND measurements remove all dependence on loss and have exchanged success probability for entanglement, while they learn that k_1-j_1 photons were lost to the environment. All outcomes besides zero at Alice and Bob herald useful entanglement. If $j_1 \neq k_1$, they must do further rounds of purification (iteration) since the output state is not pure. If $j_1 = k_1$, then the output state is strictly pure and purification is complete in a single round. For a simpler protocol, Alice and Bob may post-select on outcomes $j_1 = k_1$ without further iteration. We show later in the paper that this single-shot protocol still gives excellent rates.

Explicitly, the global output state heralded by outcomes k_1 and j_1 is

$$|\phi_{k_1,j_1,m}\rangle_{\mathrm{ABe}} = (1-\chi^2)^{\frac{m}{2}}\chi^{k_1}(1-\eta)^{\frac{k_1-j_1}{2}}\eta^{\frac{j_1}{2}}\sum_{n_1,n_2,\cdots,n_m}^{n_1+n_2+\cdots+n_m=k_1}\sum_{l_1,l_2,\cdots,l_m}^{l_1+l_2+\cdots+l_m=k_1-j_1,\, l_i\leq n_i\forall i}\sqrt{\binom{n_1}{l_1}\binom{n_2}{l_2}\binom{n_3}{l_3}\cdots\binom{n_m}{l_m}}|n_1,n_2,\cdots,n_m\rangle_{\mathrm{A}}\otimes|n_1-l_1,n_2-l_2,\cdots,n_m-l_m\rangle_{\mathrm{B}}\otimes|l_1,l_2,\cdots,l_m\rangle_e, \tag{3}$$

where A, B, e refer to the m-rail quantum systems owned by Alice, Bob, and the environment, respectively, as shown in Fig. 1. The full derivation of this state is in Supplementary Note 2. The factor $(1-\eta)^{\frac{k_1-j_1}{2}}\eta^{\frac{j_1}{2}}$ is outside the sum, thus, we have the remarkable result that the renormalised output state shared between Alice and Bob does not depend on η. Therefore, the entanglement shared between Alice and Bob also has no dependence on η, which has been exchanged for probabilities.

Additional rounds of purification can purify more entanglement after the initial round. One approach is for Alice and Bob to locally perform QND measurements as in round one but on $m-n+1$ rails, and obtain outcomes k_n, j_n, where n refers to the round number. At round n, there is no entanglement shared between Alice and Bob on the last $n-1$ rails and the photon number of each of these rails is completely known. At round n, these last $n-1$ rails can be discarded while the $m-n+1$ rails should be kept.

Rate of iterative purification for finite numbers of rails

The rate of our purification protocol (in ebits per use) is maximised if Alice performs her first measurement offline (i.e., setting $P^{\mathrm{Alice}}_{k_1,m} = 1$), where she obtains outcome k_1. For finite m, there is a finite k_1 which optimises the rate. However, for large squeezing $\chi \to 1$ outcomes k_1 is dominated by $k_1 \to \infty$ with unity probability. Therefore, the large squeezing limit $\chi \to \infty$ without k_1 pre-selection is equivalent to $k_1 \to \infty$ with offline k_1 pre-selection.

Taking Alice's first measurement to be done with result k_1 offline (which can be chosen in advance to optimise the rate or, for example, the practicality of the protocol), the rate for finite m is

$$E_{k_1,m}(\eta) = \frac{1}{m}\sum_{n=1}^{m-1}\sum_{j_1,k_2,j_2,\cdots,k_n,j_n}\mathrm{PE}, \tag{4}$$

where the sum is constrained by

$$k_1 \geq k_2 \geq k_3 \geq \cdots \geq k_n, \tag{5}$$

$$j_1 \geq j_2 \geq j_3 \geq \cdots \geq j_n, \tag{6}$$

$$k_s - k_{s+1} \geq j_s - j_{s+1}\forall s, \tag{7}$$

$$k_s > j_s \forall s \neq n, \tag{8}$$

$$k_n = j_n, \tag{9}$$

where the probability of success for a particular combination of outcomes, $j_1, k_2, j_2, \ldots, k_n, j_n$, for a given k_1 and m is

$$P = (1-\eta)^{k_1-j_1}\eta^{j_1}\frac{\binom{k_n+m-n}{k_n}\binom{k_n}{j_n}}{\binom{k_1+m-1}{k_1}}\left[\prod_{s=1}^{n-1}\binom{k_s-k_{s+1}}{j_s-j_{s+1}}\right], \tag{10}$$

where a maximally entangled state is generated with entanglement

$$E = \log_2\left[\binom{k_n+m-n}{k_n}\right]. \tag{11}$$

The rate $E_{k_1,m}(\eta)$ for finite m can be optimised over Alice's initial outcome k_1 prepared offline and the number of rails m as a function of η. We numerically compute the rate in Supplementary Note 3 for small k_1 and m. We show next that the highest rate of our iterative protocol achieves the capacity, C, for $m \to \infty$ and $k_1 \to \infty$ (i.e., $\chi \to 1$). We show this without having to compute Eq. (4) directly which would be arduous.

Optimality of our protocol

The RCI[10,13], R, gives an achievable lower bound on the distillable entanglement, E_{D}, and on the optimal secret key rate. The RCI is defined in the "Methods" section. We will show that our protocol is optimal for entanglement distillation as $m \to \infty$ and $\chi \to 1$ and that no entanglement is lost between rounds. We use the RCI as a benchmark to test the quality of our distillation procedure. The optimal distillation protocol implicit by the RCI is not required here since our scheme gives the same performance as the implicit optimal protocol round after round for large m.

We require that the weighted average von Neumann entropy of the reduced pure states heralded after round one, S_1, plus the average RCI of the failure states heralded after round one, F_1, equals the RCI of the state before round one. Note that the RCI equals the von Neumann entropy for pure states. We have

$$S_1 + F_1 = \frac{1}{m}\sum_{k_1=0}^{\infty}\sum_{j_1=0}^{k_1}P_{k_1,j_1,m}R_{k_1,j_1,m}, \tag{12}$$

in units of ebits per channel use, where

$$S_1 = \frac{1}{m}\sum_{k_1=0}^{\infty}P_{k_1,j_1=k_1,m}R_{k_1,j_1=k_1,m}, \tag{13}$$

$$F_1 = \frac{1}{m}\sum_{k_1=0}^{\infty}\sum_{j_1=0}^{k_1-1}P_{k_1,j_1,m}R_{k_1,j_1,m}, \tag{14}$$

where $P_{k_1,j_1,m} = P^{\mathrm{Alice}}_{k_1,m}P^{\mathrm{Bob}}_{k_1,j_1}$, where $P^{\mathrm{Alice}}_{k_1,m} = (1-\chi^2)^m\chi^{2k_1}d_{k_1,m}$ and $P^{\mathrm{Bob}}_{k_1,j_1} = (1-\eta)^{k_1-j_1}\eta^{j_1}\binom{k_1}{j_1}$. When the first round succeeds, the entanglement of the renormalised maximally entangled pure-state shared between Alice and Bob heralded by outcomes $k_1 = j_1$ is given by the von Neumann entropy of the reduced state:

$$E_{k_1=j_1,m} = R_{k_1,j_1=k_1,m} = \log_2\left[\binom{k_1+m-1}{k_1}\right], \tag{15}$$

which does not depend on the transmissivity, η, nor the amount of two-mode squeezing, χ. When the first round fails, the RCI of the renormalised mixed state shared between Alice and Bob heralded by each pair of outcomes k_1 and j_1 is

$$R_{k_1 j_1, m} = \log_2 \left[\frac{\binom{k_1 + m - 1}{k_1}}{\binom{k_1 - j_1 + m - 1}{k_1 - j_1}} \right], \tag{16}$$

which also does not depend on the transmissivity, η, nor the amount of two-mode squeezing, χ. See Supplementary Note 2 for the derivation.

The amount of squeezing is scaled to infinity $\chi \to 1$, such that Alice initially measures a large amount of photons $k_1 \to \infty$ and $m/k_1 \to 0$. Furthermore, from the fact that $P^{\text{Bob}}_{k_1 j_1}$ is a binomial distribution, Bob will most likely measure $j_1 \approx \eta k_1$ photons. Using these conditions, we show in Supplementary Note 3 that Eq. (12) approaches

$$\lim_{\chi \to 1} (S_1 + F_1) = -\frac{m-1}{m} \log_2 (1 - \eta) = \frac{m-1}{m} C, \tag{17}$$

which ensures that round one of purification is optimal since there is no loss of rate after round one as $m \to \infty$, given that the average RCI at the end of the round equals the initial RCI of the protocol. Thus, there exists an optimal protocol to follow round one which can saturate the two-way assisted quantum capacity (the PLOB bound) using our protocol as an initial step. The entanglement is optimally exchanged for success probability.

Similarly, we prove in Supplementary Note 3 that round n is optimal since there is no loss of rate at round n as $m \to \infty$, up to the same factor, $\frac{m-1}{m}$. This factor comes from Alice's and Bob's measurements of photon numbers.

To quantify this loss of entanglement, consider the protocol before the channel. We will see that for finite m some entanglement is immediately lost after Alice's QND measurement. Ref. [44] defined the entanglement ratio, denoted by Γ_1, as the average entanglement heralded by Alice's QND measurement divided by the total initial entanglement mE_χ, that is,

$$\Gamma_1 \equiv \frac{\sum_{k_1=0}^{\infty} P^{\text{Alice}}_{k_1, m} E_{k_1, m}}{m E_\chi}. \tag{18}$$

In the limit of a large number of rails $\lim_{m \to \infty} \Gamma_1 = 1$ for all $0 < \chi \leq 1$, which means asymptotically Alice's QND measurement heralds no loss of entanglement. However, for finite m in the limit of large squeezing, $\lim_{\chi \to 1} \Gamma_1 = (m-1)/m$. So, for a finite number of rails m some entanglement is lost since $1/2 < (m-1)/m < 1$. This means we must take $m \to \infty$ to get the highest rates.

Similarly, to quantify the entanglement lost at round $n > 1$, we define the entanglement ratio, $\Gamma_{k_{n-1}}$, as the weighted average entanglement heralded at round n overall outcomes k_n normalised by the weighted entanglement heralded by outcome k_{n-1} at the previous round, $n-1$, that is,

$$\Gamma_{k_{n-1}} \equiv \frac{\sum_{k_n} P_{k_n} E_{k_n}}{P_{k_{n-1}} E_{k_{n-1}}} = \frac{\sum_{k_n} d_{k_n} \log_2 d_{k_n}}{d_{k_{n-1}} \log_2 d_{k_{n-1}}}, \tag{19}$$

where $d_{k_n} = \binom{k_n + m - n}{k_n}$ and $d_{k_{n-1}} = \binom{k_{n-1} + m - n + 1}{k_{n-1}}$. P_{k_n} ($P_{k_{n-1}}$) and E_{k_n} ($E_{k_{n-1}}$) are defined in Eqs. (10) and (11), for a given $k_n (k_{n-1})$, and of course, we can take $j_i = k_i$ for all i since here we consider no loss channel. Many of the factors cancel giving the simple expression in Eq. (19). Curiously, for large numbers of rails, the amount of entanglement lost at round n is the same as for round one, i.e., $\lim_{m \to \infty} \Gamma_{k_{n-1}} = (m-1)/m$ for all k_{n-1}. This result ensures that "encoding" into k_n photons is asymptotically optimal throughout the entire duration of our iterative procedure up to the factor $(m-1)/m$, which approaches unity for large m.

Achieving the capacity

The average rate in case of success of pure entanglement distilled at round n in ebits per use of the channel is

$$S_n = \frac{1}{m} \sum_{k_1 j_1, \ldots, k_n j_n} \text{PE}\, \delta_{k_n j_n}, \tag{20}$$

and the average rate in case of failure of entanglement distilled at round n in ebits per use of the channel is lower bounded by the average RCI

$$F_n = \frac{1}{m} \sum_{k_1 j_1, \ldots, k_n j_n} \text{PR}\, (1 - \delta_{k_n j_n}), \tag{21}$$

where P is the probability from Eq. (10) and $R = \log_2 \left[\frac{\binom{k_n + m - n}{k_n}}{\binom{k_n - j_n + m - n}{k_n - j_n}} \right]$ is the RCI of the heralded states. Note $\delta_{k_n j_n}$ is the Kronecker delta function. For the rate in case of success, the RCI equals the von Neumann entropy since the states are pure, $R = E$. The entanglement in case of failure at round n will be purified at a later round.

Since our protocol is optimal at round n for $\chi \to 1$ and $m \to \infty$, we have the following expressions:

$$S_1 + F_1 = \frac{m-1}{m} C \tag{22}$$

$$\lim_{m \to \infty} (S_n + F_n) = \lim_{m \to \infty} \left(\frac{m-1}{m} F_{n-1} \right), \tag{23}$$

for $2 \leq n \leq m$. We solve this system of equations by addition, and we find that the average rate in case of success of purification using our iterative procedure for $m \to \infty$ and $\chi \to 1$ is

$$E_{\text{iteration}} = \lim_{m \to \infty} \sum_{n=1}^{m} S_n \tag{24}$$

$$= \lim_{m \to \infty} \frac{m-1}{m} C - \lim_{m \to \infty} \sum_{n=1}^{m-1} \frac{F_n}{m} \tag{25}$$

$$= C. \tag{26}$$

We achieve the capacity (PLOB) in the limit of a large number of rails, where $\lim_{m \to \infty} \sum_{n=1}^{m-1} \frac{F_n}{m} \to 0$ and $\lim_{m \to \infty} (m-1)/m \to 1$. See Supplementary Note 3 for the proof.

Achievable rates of repeater networks

Our protocol purifies completely at the PLOB rate. Assuming ideal quantum memories are available, after teleportation (entanglement swapping) we achieve the ultimate end-to-end rates of quantum communication networks by adopting the routing methods of ref. [15]. That is, the results can be extended beyond chains to consider more complex topologies and routing protocols[15]. We describe details about entanglement swapping in Supplementary Note 4. We plot the highest rates of iterative purification as a function of total distance with no repeater and one repeater in Fig. 2a (black lines) which coincide with the capacities. We also plot rates in Fig. 2a for single-shot purification for finite m where Alice and Bob stop after the first round which is a much more practical design. We discuss in detail those single-shot rates next.

Single-shot purification

Purification is complete after a single round if no photons are lost and Alice and Bob detect the same number of photons, $j_1 = k_1$. If Bob detects fewer photons than Alice, $j_1 < k_1$, further purification is required, however, it is most practical to disregard those

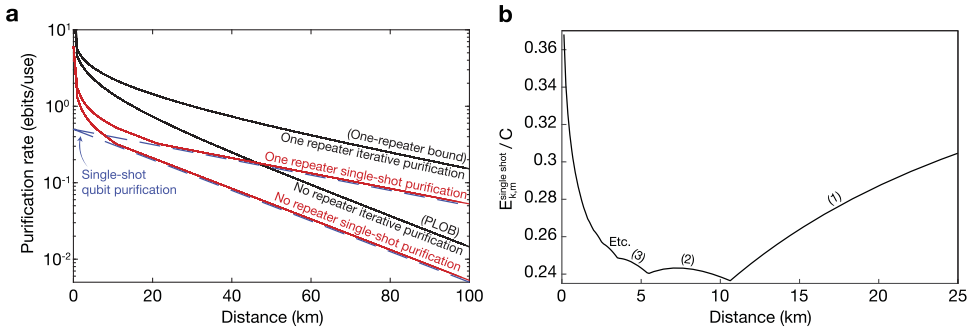

Fig. 2 Optimal rates of entanglement purification. a We plot the highest rates of iterative purification (black), single-shot purification (red), and single-shot purification for qubits (blue dashed) as a function of the total end-to-end distance, for optical fibre with a loss rate of 0.2 dB km^{-1}. Purification is used to distribute and purify entanglement between nodes and entanglement swapping connects the end users. To illustrate, we plot rates without a repeater and with one repeater. Equivalently, these rates are secret key rates since ebits are specific types of secret bits[62]. Our highest rates coincide with the ultimate limits of quantum communications (black), shown here the repeaterless PLOB bound[14] and the one-repeater bound[15]. At all distances, the output states are strictly pure. The scaling improves for increased numbers of repeaters (not shown). **b** The ratio of the optimised rate of our single-shot purification protocol without a repeater with the repeaterless PLOB bound as a function of distance, showing how close it comes to saturating the bound (and therefore end-to-end quantum-repeater networks in general). The optimal number of photons, k, at each distance is shown in rounded brackets. At shorter distances codes with more photons are optimal. The three-rail encoding ($m = 3$) is optimal at most distances, with sometimes a larger m optimal at distances less than about 1.6 km. At large distances, the ratio $E_{k,m}^{\text{single shot}}/C$ approaches $\ln(3)/3 \sim 0.366$. As the distance goes to zero, $E_{k,m}^{\text{single shot}}/C = 1/2$.

outcomes and keep only the outcome $j_1 = k_1$ which purifies in one shot. Alice's measurement can be pre-selected and prepared offline, thus, improving the rate of a particular pair of outcomes. The single-shot rate for a given m and $k \equiv k_1 = j_1$ can be quite close to the PLOB rate.

Recall that the optimal protocol implicit by the RCI is based on one-way classical communication[13], whereas, our iterative procedure requires two-way classical communication. Here, the single-shot protocol requires only one-way classical communication, like the implicit optimal protocol. Alice and Bob agree on the quantum-error-detecting code (k and m) in advance, so Alice does not need to send any classical information towards Bob. Bob only needs to send classical information towards Alice, telling her when the protocol succeeds. This greatly simplifies the required back-and-forth signalling in a quantum network.

Highest achievable rate of single-shot purification

The rate of single-shot purification is as follows. The probability that Alice obtains outcome k is $P_{k,m}^{\text{Alice}} = (1-\chi^2)^m \chi^{2k} d_{k,m}$, however, for the single-shot protocol we can incorporate this step into Alice's state preparation and assume this is done offline such that $P_{k,m}^{\text{Alice}} = 1$. This means the rate will not depend on χ. When Bob obtains the outcome which matches Alice's, k, his probability is $P_k^{\text{Bob}} = \eta^k$ and the output state is pure with entanglement $E_{k,m} = \log_2 d_{k,m}$. Thus, the achievable rate of single-shot entanglement purification in ebits per use of the channel is

$$E_{k,m}^{\text{single shot}}(\eta) = \frac{P_k^{\text{Bob}} E_{k,m}}{m} = \frac{\eta^k}{m} \log_2 \binom{k+m-1}{k}. \tag{27}$$

The rate is divided by the number of rails, m, to compare directly with the PLOB bound[14]. This is required because Alice and Bob exploit a quantum channel whose single use involves the simultaneous transmission of m distinct systems in a generally entangled state.

This rate is for a perfect implementation without any additional losses, errors, or noise. The protocol heralds pure states in a single attempt, so if we have ideal quantum memories, after entanglement swapping (see Supplementary Note 4 for details on entanglement swapping) we can distribute entanglement between ends of a network without any loss of rate, i.e., at the rate given by Eq. (27) where η is the transmissivity of the most destructive link.

Our optimised rate over k and m is shown in Fig. 2a, without and with one quantum repeater (with a repeater, we assume ideal quantum memories). The PLOB bound can ultimately be broken at 46.3 km using single-shot purification between nodes and a single repeater for entanglement swapping. In Fig. 2b, we show the ratio of our optimised single-shot rate with the PLOB bound, showing that at long distances the protocol falls short of the PLOB bound by just a factor of $\ln(3)/3 \sim 0.366$, and remarkably, our rate approaches $C/2$ at short distances. At short distances, the rate is optimised for larger k while at long distances $k = 1$ is always optimal since the probability that photons arrive scales like η^k at long distances. The optimal number of rails is about $m = 3$ at most distances (including long distances) since increasing the number of rails decreases the rate like $1/m$. Larger m is sometimes optimal at short distances.

The rate of our single-shot purification protocol is unable to saturate the ultimate limit because we post-select on Bob's outcomes, throwing away useful entanglement when $j \neq k$ and $j > 0$. Keeping all measurement outcomes, the rate increases, however, it is less practical to do so.

Quantum error detection

In this section, we describe our single-shot purification protocol as quantum error detection. Consider encoding an arbitrary finite-dimensional single-rail state with dimension $d_{k,m}$:

$$|\psi_{k,m}\rangle = \frac{1}{\sqrt{N_\psi}} \sum_{\mu=0}^{d_{k,m}-1} c_\mu |\mu\rangle, \tag{28}$$

where $N_\psi = \sum_{\mu=0}^{d_{k,m}-1} |c_\mu|^2$.

The code is a subspace with $d_{k,m}$ dimensions ($d_{k,m}$-dimensional), a subspace of the infinite-dimensional Hilbert space chosen to detect loss errors nondeterministically. It is represented by the projector onto the subspace

$$\mathcal{P}_{k,m} = \sum_{\mu=0}^{d_{k,m}-1} |\mu_{k,m}\rangle\langle\mu_{k,m}|, \tag{29}$$

where $|\mu_{k,m}\rangle = |n_1^{(\mu)}, n_2^{(\mu)}, n_3^{(\mu)}, \cdots, n_m^{(\mu)}\rangle$ are the orthogonal basis states (code words) which make up the code subspace (code space), where μ is the logical label. Note $n_i^{(\mu)}$ is the number of photons in the ith rail, which depends on the logical label μ, as well as k and m where $\sum_{i=1}^m n_i^{(\mu)} = k$. There are $d_{k,m}$ code words,

i.e., for a given code the set of code words is $\{|\mu_{k,m}\rangle\} = \{|0_{k,m}\rangle, |1_{k,m}\rangle, |2_{k,m}\rangle, \cdots\}$. Quantum information up to dimension $d_{k,m}$ can faithfully be transmitted to Bob, conditioned that he detects no errors. Photon loss (and photon gains) will result in states outside of code space, which we can distinguish as an error.

The set of logical states forming the $d_{k,m}$-dimensional basis of the code consists of all possible ways k identical photons can be arranged among the m distinct rails. For example, $|\mu_{k=2,m=3}\rangle \in \{|0,0,2\rangle, |0,2,0\rangle, |2,0,0\rangle, |0,1,1\rangle, |1,0,1\rangle, |1,1,0\rangle\}$. The code space is a subspace of the full Hilbert space of the m rails which introduces the redundancy required for error detection, that is, k photons and m rails can encode $d_{k,m}$-dimensional states. The dimension grows rapidly with k and m. For example, with just $k = 4$ photons and $m = 5$ rails, we can efficiently encode 70-dimensional states, i.e., truncated at Fock number $|69\rangle$, with success probability $P^{\text{Bob}}_{j=k=4} = \eta^k = \eta^4$. This is a great advantage over noiseless linear amplification, for example, if we choose the gain of the amplifier to be $g = 1/\sqrt{\eta}$ to overcome the loss then the success probability is $P_{\text{NLA}} = 1/g^{2(d_{k,m}-1)} = \eta^{(d_{k,m}-1)} = \eta^{69}$, totally impractical. Furthermore, noiseless linear amplification fails to purify completely and cannot completely overcome the loss.

The encoding step is

$$\mathcal{S} = \sum_{\mu=0}^{d_{k,m}-1} |\mu_{k,m}\rangle\langle\mu|, \tag{30}$$

which maps Fock states, $|\mu\rangle$, from a single mode to the code words, $|\mu_{k,m}\rangle = |n_1^{(\mu)}, n_2^{(\mu)}, \cdots, n_m^{(\mu)}\rangle$. The combined operation of encoding, loss, and decoding is a completely-positive trace-non-increasing map

$$\mathcal{E} = \mathcal{S}^{-1} \circ \mathcal{L}^{\otimes m} \circ \mathcal{S} = \mathcal{E} = \eta^{k/2} \sum_{\mu=0}^{d_{k,m}-1} |\mu\rangle\langle\mu|, \tag{31}$$

where $\mathcal{L}^{\otimes m}$ is the map for independent applications of the pure-loss channel on the m rails, the decoding step, $\mathcal{S}^{-1}$, performs a QND measurement of the total photon number, and if k photons arrive, then it successfully decodes back to a single rail. The decoding step succeeds only if no photons are lost. The combined operation, $\mathcal{E}$, is a scaled identity map up to the $(d_{k,m}-1)$th Fock state, thus, the protocol succeeds with success probability $P^{\text{Bob}}_k = \text{tr}(\rho_{\text{AB}}) = \eta^k$ with unit fidelity.

The input state may be entangled with another mode. For example, we may consider encoding one arm of an arbitrary entangled state, $|\psi_{k,m}\rangle \propto \sum_{\mu=0}^{d_{k,m}-1} c_\mu |\mu\rangle_{\text{A}} |\mu\rangle_{\text{B}}$. In this case, the operation, $\mathcal{E}$, acts on Bob's mode only and Alice leaves her mode alone. The final state shared between Alice and Bob is $\rho_{\text{AB}} = (\mathbb{1} \otimes \mathcal{E})\rho_{\text{in}}$, where ρ_{in} is the initial state and $\mathbb{1}$ is the identity on mode A. Note there is still useful entanglement if photons are lost. The entanglement-distribution rate of single-shot error detection for a maximally entangled initial state $|\phi_{k,m}\rangle_{\text{AB}} = \frac{1}{\sqrt{d_{k,m}-1}} \sum_{\mu=0}^{d_{k,m}-1} |\mu\rangle_{\text{A}} |\mu\rangle_{\text{B}}$ is given by Eq. (27), showing that error detection and purification indeed are equivalent.

One might consider using purification to distribute Gaussian entanglement for long-distance CV QKD between trusted end users of a network, performing the entanglement-based CV-QKD protocol based on homodyne detection[45,46] or heterodyne detection[47]. Consider the initial data state to be a truncated TMSV state with dimension $d_{k,m}$ given by

$$|\chi_{k,m}\rangle = \sqrt{\frac{\chi^2 - 1}{\chi^{2d_{k,m}} - 1}} \sum_{\mu=0}^{d_{k,m}-1} \chi^\mu |\mu\rangle_{\text{A}} |\mu\rangle_{\text{B}}. \tag{32}$$

The state is Gaussian except for the hard truncation in Fock space. The protocol works as follows. First, truncated TMSV states, $|\chi_{k,m}\rangle$, are distributed using our single-shot purification scheme between all repeater nodes and held in quantum memories. Once successful, CV entanglement swapping is used to entangle the end users who use the entanglement to perform CV QKD. While the purification scheme can be complex (depending on the chosen protocol size), the CV entanglement swapping is simple. It works by performing dual-homodyne measurements on some of the modes, followed by conditional displacements, swapping the entanglement[48], see Supplementary Note 4 for details on how to compute the secret key rate.

A simple example: the qubit code

The simplest nontrivial code uses a single photon, $k = 1$, in two rails, $m = 2$, (i.e., unary dual-rail) and protects qubit systems, $d_{k=1,m=2} = 2$, from loss. It is equivalent to the original purification protocol from ref. [43], but in this context, we use it to purify entanglement completely from pure loss to first order in Fock space and we can protect arbitrary single-rail qubit states from loss. The code words can be defined $|0_{k=1,m=2}\rangle \equiv |0,1\rangle$ and $|1_{k=1,m=2}\rangle \equiv |1,0\rangle$. The projector onto the code space is $\mathcal{P} = |0,1\rangle\langle 0,1| + |1,0\rangle\langle 1,0|$. The encoding step is

$$\mathcal{S} = |0_{k=1,m=2}\rangle\langle 0| + |1_{k=1,m=2}\rangle\langle 1| \tag{33}$$

$$= |0,1\rangle\langle 0| + |1,0\rangle\langle 1|, \tag{34}$$

which maps the vacuum component of the data mode onto a single photon of the second rail and the single-photon component of the data mode onto a single photon of the first rail. If either of these photons is lost, the protocol fails. The success probability is $P^{\text{Bob}}_{j=k=1} = \eta$. The maximum single-shot rate in ebits per use is $D^{\text{single shot}}_{k=1,m=2}(\eta) = \eta/2$, as shown by the dashed line in Fig. 2a (with and without a repeater).

Physical implementation

Entanglement purification (iterative and single shot) requires joint QND measurements on multiple rails. These measurements can be performed via controlled-SUM quantum gates and photon number-resolving measurements (see Supplementary Note 5, for example). Another technique is to use high finesse cavities and cross-Kerr nonlinearities[44].

More simply, our scheme can be implemented using beamsplitters and photon-number-resolving detectors, however, it also requires an entangled resource state, $|\Omega_{k,m}\rangle$. This is a common technique in linear optics[49,50]. See ref. [51] for a review of quantum information processing using linear optics. The resource state can also be generated using linear optics and photon-number measurements. That is, we have a simple method of implementing our protocol, though at some cost to the success probability.

We focus on the single-shot linear-optics protocol, shown in Fig. 3. Alice shares m entangled states, $|\chi\rangle$, with Bob. Note each rail could have a different χ, distiling different amounts of entanglement between Alice and Bob at the end of the protocol, however, maximal entanglement is heralded when all rails have the same value of χ. Alice and Bob each prepare locally multimode resource states, $|\Omega_{k,m}\rangle$, consisting of $(m+1)$ modes. We assume they do this offline so it does not affect the quantum communication rate:

$$|\Omega_{k,m}\rangle \propto \sum_{\mu=0}^{d_{k,m}-1} f_\mu |\mu\rangle |\mu_{\widetilde{k,m}}\rangle, \tag{35}$$

where $|\mu\rangle$ are Fock states, $|\mu_{\widetilde{k,m}}\rangle$ are "anticorrelated" code words. Writing the usual code words in the Fock basis as $|\mu_{k,m}\rangle = |n_1^{(\mu)}, n_2^{(\mu)}, n_3^{(\mu)}, \cdots, n_m^{(\mu)}\rangle$, where $n_i^{(\mu)}$ is the number of

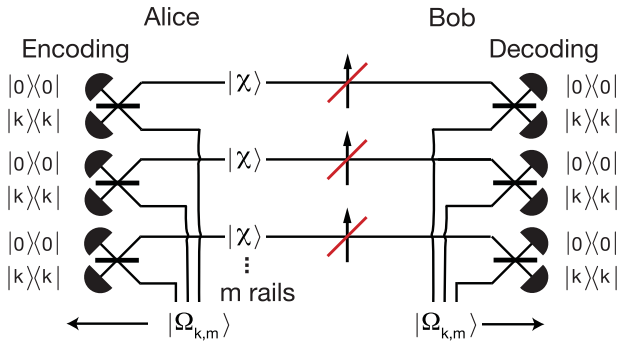

Fig. 3 Implementation using linear optics and number measurements. The aim of the protocol is for Alice to share quantum information contained in a $d_{k,m}$-dimensional pure state, $|\psi_{k,m}\rangle$, which can be entangled with another system which Alice keeps, with Bob separated by a pure-loss channel. Shown in this figure, the aim is to distribute a pure maximally entangled state between Alice and Bob. Alice shares m entangled states, $|\chi\rangle$, with Bob. Encoding/decoding simply requires beamsplitters, photon detectors, and $(m+1)$-mode entangled resource states, $|\Omega_{k,m}\rangle$. We can assume Alice's encoding (the state heralded after Alice's measurement) is prepared offline so that the success probability of the protocol is the probability of Bob's side only. There is, however, a success-probability penalty for using linear optics, noting crucially that this penalty does not depend on the loss. The protocol succeeds when Bob detects the same number of photons Alice sent, k. If Bob detects less photons, multiple rounds of error detection are required or Alice and Bob can simply disregard those states.

photons in the ith rail, and where $\sum_{i=1}^{m} n_i^{(\mu)} = k$, recalling that the code space was defined as the set of all states with this property, then $|\mu_{\widetilde{k,m}}\rangle = |k - n_1^{(\mu)}, k - n_2^{(\mu)}, k - n_3^{(\mu)}, \cdots, k - n_m^{(\mu)}\rangle$. The coefficients, f_n, are

$$f_n = \left[\binom{k}{n_1^{(\mu)}}\binom{k}{n_2^{(\mu)}}\cdots\binom{k}{n_m^{(\mu)}}\right]^{-1/2}. \tag{36}$$

The last m modes of $|\Omega_{k,m}\rangle$ are fed into the beamsplitters with the distributed entanglement and are measured by photon-number detectors. The first mode is kept locally by the user and remains at the end of the protocol, as shown in Fig. 3.

Detecting k photons means there were no loss events since $n_i^{(\mu)} + k - n_i^{(\mu)} = k$. That is, all photons are accounted for in the circuit and the output state is strictly pure. There may be useful entanglement for measurement outcomes other than $|0,k\rangle\langle 0,k|$ at each pair of detectors, and further purification (iteration) can increase the rate, but we do not consider it due to practicality.

Adjusting the amount of entanglement prepared for each rail, adjusting the loss on each rail, or selecting different coefficients in the resource state, f_n, results in a different output state, which may be useful for certain tasks. For example, if the entangled states prepared for each rail are identical and have the same amount of squeezing and f_n is chosen as in Eq. (36), then a maximally entangled state will be heralded between Alice and Bob at the output. For another example, consider the dual-rail case ($m = 2$), if the second rail is maximally entangled and f_n is chosen as in Eq. (36), then the output state is the initial state of the top rail. This tuning of the circuit parameters is useful, for instance, for CV QKD where the target state is a truncated TMSV state.

The linear-optics scheme detects all errors and outputs a pure state. There is, however, an additional success probability penalty using linear optics because of Bob's decoding measurement. We assume Alice prepares offline, then the success probability is

$$P_{k,m}^{\text{Bob linear optics}} = \frac{\eta^k}{2^{m(k-1)}\sum_{n=0}^{d-1} f_n^2}, \tag{37}$$

which depends on m. Compare this with the ideal purification protocol where $P_k^{\text{Bob}} = \eta^k$ which does not depend on m. The penalty paid for using linear optics is mainly due to the exponential $2^{m(k-1)}$ factor, which is painful for anything other than $k = 1$, where $P_{k=1}^{\text{Bob linear optics}} = \eta/m$. For more details we refer you to Supplementary Note 6.

The linear-optics circuit leads naturally to a controlled-SUM gate using linear optics and number measurements, albeit with distorted coefficients (this distortion ultimately has no effect in our protocol since we immediately measure the state). For the interested reader, we refer you to Supplementary Note 5 for more details.

Since Alice's encoded state is prepared offline, it is useful to consider more generally that she encodes an arbitrary state into the code: $(\mathbb{1} \otimes \mathcal{S})|\psi_{k,m}\rangle$.

Preparation of resource states

For our linear optics and number measurement circuit, the resource state, $|\Omega_{k,m}\rangle$, and Alice's encoded state she prepares offline, are multi-mode entangled states. Once these states are prepared, our scheme requires just beamsplitters and photon detectors. One practical way to prepare these states is to use a Gaussian Boson Sampler (GBS)[52] and post-selecting on a specific photon-number-resolving measurement click pattern on some of the modes of the output[53,54]. This allows our scheme to be implemented entirely using linear optics and number measurements. Using the GBS method for the simplest scheme with $k = 1$ and $m = 2$, we have found the resource state, $|\Omega_{k=1,m=2}\rangle = (|0,1,0\rangle + |1,0,1\rangle)/\sqrt{2}$, can be prepared with high fidelity, $F > 0.999$, with success probability $\approx 10^{-6}$. This was found by optimising the parameters of a GBS network via a machine learning algorithm called "basin hopping"[55]. In https://github.com/JGuanzon/state-finder, we have provided our code that implements this algorithm, as well as the parameter set we found that generates this resource state. Alternatively, adaptive phase measurements[56] can be used to prepare the needed resource states directly from dual-rail Bell pairs or GHZ-like states which may have a higher probability of success.

Experimental imperfections

Our linear-optics circuit is robust to loss. The quality of the state Alice sends can be managed since her encoding is done offline. In any case, we are interested in the noise introduced by the protocol, not the noise in the initial state we are trying to transmit. The measurement and detection scheme at Bob's side is such that all photons are accounted for, so if Alice's encoding is perfect, the protocol can correctly identify if any photons are lost in the channel or at the detectors. More details are presented in Supplementary Note 6, where we also perform a numerical simulation incorporating inefficient detectors with dark counts and a thermal-noise channel. Our protocol is robust to the practical values of these imperfections.

The directionality issue

Often in quantum communications, it is best if quantum states propagate in one preferred direction (from Alice towards Bob) when reverse reconciliation is used. This is a persistent problem in CV quantum communications. For instance, CV measurement-device-independent protocols[57–60] work only in an extremely asymmetric configuration, with the node (ineffective as a repeater) positioned close to one of the trusted parties. This directionality problem is also present in the repeater protocols

considered in ref. [29,30], where they work best in one direction, which for reverse reconciliation is again from Alice towards Bob. Our purification schemes allow states to propagate in any direction in a quantum network since the output states are pure. Using purification for CV-QKD works the same for both direct and reverse reconciliations. We have no directionality problem. This is an important requirement for large CV networks. Note that the memoryless CV repeater protocol introduced in ref. [31] also fixes the directionality problem.

DISCUSSION

We have presented a physical protocol that achieves the two-way assisted quantum capacity of the pure-loss channel[14]. Error correction requires short distances between neighbouring repeater nodes, while in contrast, we showed simple error detection can saturate the PLOB bound. An open question is what protocol can saturate the fundamental limits for added thermal noise and close the gap between the theoretical upper and lower bounds[14].

Our protocol is an optimal one and can be performed using CSUM quantum gates and measurements. However, it is unknown whether other gates and measurements may also achieve the capacity, and if they can do so more efficiently, i.e., approaching the PLOB bound more quickly with the number of iteration rounds, n.

Our ultimate protocol is experimentally challenging since it requires iterative purification steps. However, we show that by simplifying our protocol to just a single round of purification, we can still achieve excellent rates. This is superior to other nondeterministic techniques such as noiseless linear amplification where it is impossible to remove all effects of loss.

Our purification protocol can be implemented using linear optics and number measurements. This does introduce some probability penalty (which does not depend on the loss), however, having an all-optical design is experimentally convenient.

One limitation of our results is the requirement for high-performance quantum memories. However, purification outputs pure states which is extremely beneficial. Firstly, pure states can handle a higher amount of decoherence coming from nonideal quantum memories. Secondly, distributing pure states will prevent how much thermal noise builds up across a network during entanglement swapping. Finally, purity may be beneficial for both point-to-point and repeater-assisted CV QKD, improving the signal-to-noise ratio and decreasing Eve's knowledge of the key, speeding up the classical post-processing part of the protocol.

Thus, purification is inherently a useful technique for overcoming the unavoidable losses in quantum communication networks. Remarkably, purification can be employed totally using linear optics and number measurements and is compatible with existing DV and CV infrastructure. Finally, we remark that since the lossy entanglement is completely purified, it can be used for exotic tasks, such as device-independent quantum key distribution and demonstrating Bell nonlocalities, over long distances.

METHODS

Noise model

Bosonic pure loss is the dominant source of noise for many quantum communication tasks. The pure-loss channel is equivalent to introducing a vacuum mode and mixing the data state on a beamsplitter with transmissivity $\eta \in [0, 1]$. The Kraus-operator representation of the single-mode pure-loss channel is[61]

$$\mathcal{L}(\rho) = \sum_{l=0}^{\infty} A_l \rho A_l^{\dagger}, \tag{38}$$

with Kraus operators $A_l = \sqrt{\frac{(1-\eta)^l}{l!}} \eta^{\frac{\hat{n}}{2}} \hat{a}^l$ associated with losing l photons to the environment, where $\hat{a}$ and $\hat{a}^{\dagger}$ are the single-mode annihilation and creation operators, respectively, and $\hat{n} = \hat{a}^{\dagger}\hat{a}$ is the photon-number operator.

Reverse coherent information

Take a maximally entangled state of two systems A and B. Propagating the B system through the quantum channel defines the Choi state of the channel. Then the reverse coherent information represents a lower bound for the distillable entanglement and for the optimal secret key rate. The reverse coherent information of a state ρ_{AB} is defined as[13]

$$R(\rho_{AB}) = S(\rho_A) - S(\rho_{AB}), \tag{39}$$

where $S(\rho_A)$ and $S(\rho_{AB})$ are von Neumann entropies of $\rho_A = \mathrm{tr}_B(\rho_{AB})$ and ρ_{AB} respectively. The von Neumann entropy of ρ is $-\mathrm{tr}(\rho \log_2 \rho)$.

DATA AVAILABILITY

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

Received: 25 March 2022; Accepted: 14 October 2022;
Published online: 08 November 2022

REFERENCES

1. Gisin, N. & Thew, R. Quantum communication. *Nat. Photonics* **1**, 165–171 (2007).
2. Cerf, N., Leuchs, G. & Polzik, E. *Quantum Information with Continuous Variables of Atoms and Light* (Imperial College Press, 2007).
3. Proctor, T. J., Knott, P. A. & Dunningham, J. A. Multiparameter estimation in networked quantum sensors. *Phys. Rev. Lett.* **120**, 080501 (2018).
4. Ge, W., Jacobs, K., Eldredge, Z., Gorshkov, A. V. & Foss-Feig, M. Distributed quantum metrology with linear networks and separable inputs. *Phys. Rev. Lett.* **121**, 043604 (2018).
5. Zhuang, Q., Zhang, Z. & Shapiro, J. H. Distributed quantum sensing using continuous-variable multipartite entanglement. *Phys. Rev. A* **97**, 032329 (2018).
6. Van Meter, R. & Devitt, S. J. The path to scalable distributed quantum computing. *Computer* **49**, 31–42 (2016).
7. Danos, V., D'Hondt, E., Kashefi, E. & Panangaden, P. Distributed measurement-based quantum computation. *Electron. Notes Theor. Comput. Sci.* **170**, 73–94 (2007). *Proceedings of the 3rd International Workshop on Quantum Programming Languages (QPL 2005).*
8. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012–1236 (2020).
9. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
10. Pirandola, S., García-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **102**, 050503 (2009).
11. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
12. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
13. García-Patrón, R., Pirandola, S., Lloyd, S. & Shapiro, J. H. Reverse coherent information. *Phys. Rev. Lett.* **102**, 210501 (2009).
14. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
15. Pirandola, S. End-to-end capacities of a quantum communication network. *Commun. Phys.* **2**, 51 (2019).
16. Munro, W. J., Azuma, K., Tamaki, K. & Nemoto, K. Inside quantum repeaters. *IEEE J. Sel. Top. Quantum Electron.* **21**, 78–90 (2015).
17. Muralidharan, S. et al. Optimal architectures for long distance quantum communication. *Sci. Rep.* **6**, 20463 (2016).
18. Giedke, G. & Ignacio Cirac, J. Characterization of gaussian operations and distillation of Gaussian states. *Phys. Rev. A* **66**, 032316 (2002).
19. Eisert, J., Scheel, S. & Plenio, M. B. Distilling gaussian states with gaussian operations is impossible. *Phys. Rev. Lett.* **89**, 137903 (2002).
20. Namiki, R., Gittsovich, O., Guha, S. & Lütkenhaus, N. Gaussian-only regenerative stations cannot act as quantum repeaters. *Phys. Rev. A* **90**, 062316 (2014).

21. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information*: 10th Anniversary Edition (Cambridge University Press, USA, 2011).
22. Braunstein, S. L. & van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513–577 (2005).
23. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).
24. Serafini, A. *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, 2017).
25. Kumar, R., Qin, H. & Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. *New J. Phys.* **17**, 043027 (2015).
26. Dias, J. & Ralph, T. C. Quantum repeaters using continuous-variable teleportation. *Phys. Rev. A* **95**, 022312 (2017).
27. Furrer, F. & Munro, W. J. Repeaters for continuous-variable quantum communication. *Phys. Rev. A* **98**, 032335 (2018).
28. Seshadreesan, K. P., Krovi, H. & Guha, S. Continuous-variable quantum repeater based on quantum scissors and mode multiplexing. *Phys. Rev. Res.* **2**, 013310 (2020).
29. Ghalaii, M. & Pirandola, S. Capacity-approaching quantum repeaters for quantum communications. *Phys. Rev. A* **102**, 062412 (2020).
30. Dias, J., Winnel, M. S., Hosseinidehaj, N. & Ralph, T. C. Quantum repeater for continuous-variable entanglement distribution. *Phys. Rev. A* **102**, 052425 (2020).
31. Winnel, M. S., Guanzon, J. J., Hosseinidehaj, N. & Ralph, T. C. Overcoming the repeaterless bound in continuous-variable quantum communication without quantum memories. Preprint at *bioRxiv* https://arxiv.org/abs/2105.03586 (2021).
32. Ralph, T. C. & Lund, A. P. Nondeterministic noiseless linear amplification of quantum systems. *AIP Conf. Proc.* **1110**, 155–160 (2009).
33. Winnel, M. S., Hosseinidehaj, N. & Ralph, T. C. Generalized quantum scissors for noiseless linear amplification. *Phys. Rev. A* **102**, 063715 (2020).
34. Guanzon, J. J., Winnel, M. S., Lund, A. P. & Ralph, T. C. Ideal quantum teleamplification up to a selected energy cutoff using linear optics. *Phys. Rev. Lett.* **128**, 160501 (2022).
35. Fiurášek, J. Teleportation-based noiseless quantum amplification of coherent states of light. *Opt. Express* **30**, 1466–1489 (2022).
36. Blandino, R. et al. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A* **86**, 012327 (2012).
37. McMahon, N. A., Lund, A. P. & Ralph, T. C. Optimal architecture for a nondeterministic noiseless linear amplifier. *Phys. Rev. A* **89**, 023846 (2014).
38. Blandino, R., Barbieri, M., Grangier, P. & Tualle-Brouri, R. Heralded noiseless linear amplification and quantum channels. *Phys. Rev. A* **91**, 062305 (2015).
39. Pandey, S., Jiang, Z., Combes, J. & Caves, C. M. Quantum limits on probabilistic amplifiers. *Phys. Rev. A* **88**, 033852 (2013).
40. Fowler, A. G. et al. Surface code quantum communication. *Phys. Rev. Lett.* **104**, 180503 (2010).
41. Gottesman, D., Kitaev, A. & Preskill, J. Encoding a qubit in an oscillator. *Phys. Rev. A* **64**, 012310 (2001).
42. Noh, K., Albert, V. V. & Jiang, L. Quantum capacity bounds of gaussian thermal loss channels and achievable rates with Gottesman–Kitaev–Preskill codes. *IEEE Trans. Inf. Theory* **65**, 2563–2582 (2019).
43. Bennett, C. H. et al. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76**, 722–725 (1996).
44. Duan, L.-M., Giedke, G., Cirac, J. I. & Zoller, P. Entanglement purification of gaussian continuous variable quantum states. *Phys. Rev. Lett.* **84**, 4002–4005 (2000).
45. J. Cerf, N., Lévy, M. & Van Assche, G. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A* **63**, 052311 (2001).
46. Gottesman, D. & Preskill, J. Secure quantum key distribution using squeezed states. *Phys. Rev. A* **63**, 022309 (2001).
47. Weedbrook, C. et al. Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).
48. Hoelscher-Obermaier, J. & van Loock, P. Optimal gaussian entanglement swapping. *Phys. Rev. A* **83**, 012319 (2011).
49. Yan, P.-S., Zhou, L., Zhong, W. & Sheng, Y.-B. Feasible measurement-based entanglement purification in linear optics. *Opt. Express* **29**, 9363–9384 (2021).
50. Yan, P.-S., Zhou, L., Zhong, W. & Sheng, Y.-B. Measurement-based entanglement purification for entangled coherent states. *Front. Phys.* **17**, 21501 (2021).
51. Kok, P. et al. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.* **79**, 135–174 (2007).
52. Hamilton, C. S. et al. Gaussian boson sampling. *Phys. Rev. Lett.* **119**, 170501 (2017).
53. Su, D., Myers, C. R. & Sabapathy, K. K. Conversion of gaussian states to non-gaussian states using photon-number-resolving detectors. *Phys. Rev. A* **100**, 052301 (2019).
54. Quesada, N. et al. Simulating realistic non-gaussian state preparation. *Phys. Rev. A* **100**, 022341 (2019).
55. Sabapathy, K. K., Qi, H., Izaac, J. & Weedbrook, C. Production of photonic universal quantum gates enhanced by machine learning. *Phys. Rev. A* **100**, 012326 (2019).
56. Ralph, T. C., Lund, A. P. & Wiseman, H. M. Adaptive phase measurements in linear optical quantum computation. *J Opt B Quantum Semiclass. Opt.* **7**, S245–S249 (2005).
57. Ma, X.-C., Sun, S.-H., Jiang, M.-S., Gui, M. & Liang, L.-M. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 042335 (2014).
58. Zhang, Y.-C. et al. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. *Phys. Rev. A* **90**, 052325 (2014).
59. Ottaviani, C., Spedalieri, G., Braunstein, S. L. & Pirandola, S. Continuous-variable quantum cryptography with an untrusted relay: detailed security analysis of the symmetric configuration. *Phys. Rev. A* **91**, 022320 (2015).
60. Pirandola, S. et al. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **9**, 397–402 (2015).
61. Chuang, I. L., Leung, D. W. & Yamamoto, Y. Bosonic quantum codes for amplitude damping. *Phys. Rev. A* **56**, 1114–1125 (1997).
62. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. Secure key from bound entanglement. *Phys. Rev. Lett.* **94**, 160502 (2005).

ACKNOWLEDGEMENTS

We thank Ozlem Erkilic, Sebastian Kish, Ping Koy Lam, Syed Assad, Deepesh Singh, and Josephine Dias for valuable discussions during this investigation. We thank Deepesh Singh for the alternative proof given in Supplementary Note 7. This research was supported by the Australian Research Council (ARC) under the Centre of Excellence for Quantum Computation and Communication Technology (CE170100012).

AUTHOR CONTRIBUTIONS

M.W. and J.J.G. conceived the idea. T.R. supervised the research and actively contributed to the discussions. N.H. provided important feedback on the manuscript and security considerations. M.W. and J.J.G. prepared the manuscript. M.W. prepared the figures and did the simulations for the numerical data. J.J.G. derived many of the analytical results including the success probability linear-optics closed expressions, and implemented the "basin hopping" algorithm for resource state preparation. All authors read and contributed to the paper.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-022-00641-0.

Correspondence and requests for materials should be addressed to Matthew S. Winnel.

Reprints and permission information is available at http://www.nature.com/reprints

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